

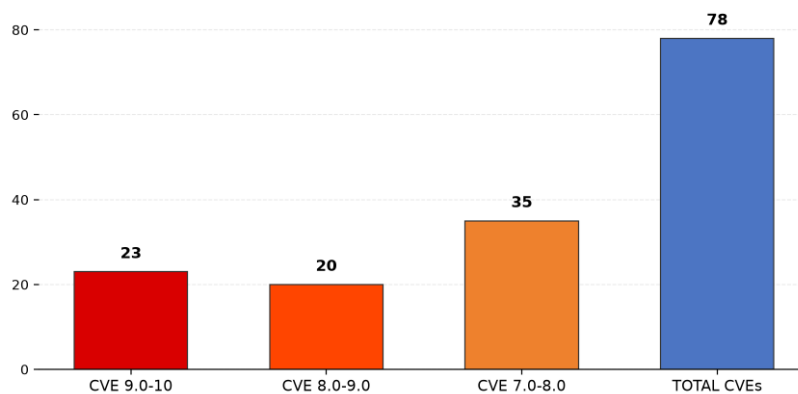


Newsletter on system vulnerabilities and cybersecurity news.

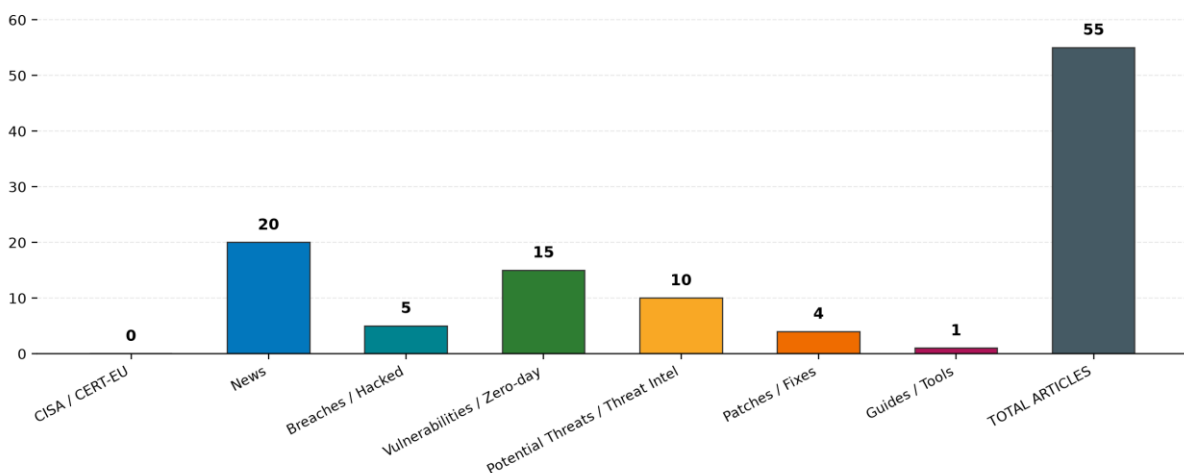
National Cyber Security Authority (NCSA)

Date: 05/09/2026 - 08/09/2026

# of CVEs per CVSS score



# of articles per section



## Contents

|                                                             |    |
|-------------------------------------------------------------|----|
| Common Vulnerabilities and Exposures (CVEs) .....           | 3  |
| CISA/CERT-EU Alerts & Advisories.....                       | 13 |
| News.....                                                   | 13 |
| Breaches / Compromised / Hacked.....                        | 14 |
| Vulnerabilities / Flaws / Zero-day.....                     | 15 |
| Patches / Updates / Fixes .....                             | 16 |
| Potential threats / Threat intelligence .....               | 16 |
| Guides / Tools.....                                         | 17 |
| References.....                                             | 18 |
| Annex - Websites with vendor specific vulnerabilities ..... | 19 |

## Common Vulnerabilities and Exposures (CVEs)

Η ενότητα αυτή εστιάζει σε ευπάθειες που έχουν καταχωρηθεί πρόσφατα και αξιολογούνται ως σοβαρές, με βάση τη βαθμολογία CVSS. Παρουσιάζονται με σαφήνεια τα συστήματα ή εφαρμογές που επηρεάζονται, ο τύπος όπως ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                                                                                                                                                                                     | Τύπος Ευπάθειας                                                                                                                                                                         | Συσκευές/Εκδόσεις που επηρεάζονται                                                                                                                                                                                                                                                 | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-44756</a> | 10,0      | the Extended Passport Protocol (EPP) processing library                                                                                                                                                             | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')                                                                                                                  | KRNL64NUC 7.22; 7.22EXT; KRNL64UC 7.22; 7.53; 8.04; WEB-DISP 9.16; 9.18; 9.19; 9.20; KER-NEL 7.22; 7.54; 7.77; 7.89; 7.93; 9.16                                                                                                                                                    | <a href="https://me.sap.com/notes/3747649">https://me.sap.com/notes/3747649</a><br><a href="https://url.sap/sapsecuritypatchday">https://url.sap/sapsecuritypatchday</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |              |             |                  |
| <a href="#">CVE-2026-75650</a> | 10,0      | Adobe Commerce                                                                                                                                                                                                      | Improper Neutralization of Special Elements Used in a Template Engine                                                                                                                   | 2.4.9-2026-aug, 2.4.8-2026-aug, 2.4.7-2026-aug, 2.4.6-2026-aug, 2.4.5-2026-aug, 2.4.4-2026-aug and earlier; 1.5.3-2026-aug, 1.5.2-2026-aug, 1.4.2-2026-aug, 1.3.4-2026-aug, 1.3.3-2026-aug and earlier; 2.4.9-2026-aug, 2.4.8-2026-aug, 2.4.7-2026-aug, 2.4.6-2026-aug and earlier | <a href="https://helpx.adobe.com/security/products/magento/apsb26-146.html">https://helpx.adobe.com/security/products/magento/apsb26-146.html</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |              |             |                  |
| <a href="#">CVE-2026-86152</a> | 10,0      | Tenda CP3                                                                                                                                                                                                           | Improper Neutralization of Special Elements used in a Command ('Command Injection'); Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')         | 27.5.57.101                                                                                                                                                                                                                                                                        | <a href="https://vuldb.com/cve/CVE-2026-86152">https://vuldb.com/cve/CVE-2026-86152</a><br><a href="https://vuldb.com/submit/895353">https://vuldb.com/submit/895353</a><br><a href="https://vuldb.com/vuln/399275">https://vuldb.com/vuln/399275</a><br><a href="https://vuldb.com/vuln/399275/cti">https://vuldb.com/vuln/399275/cti</a><br><a href="https://www.tenda.com.cn/">https://www.tenda.com.cn/</a>                                                                                                                                                                                                                                                                              |              |             |                  |
| <a href="#">CVE-2026-86296</a> | 10,0      | D-Link DIR-822A A_101                                                                                                                                                                                               | Improper Restriction of Operations within the Bounds of a Memory Buffer; Stack-based Buffer Overflow                                                                                    | A_101                                                                                                                                                                                                                                                                              | <a href="https://tzh00203.notion.site/D-Link-DIR-822A-Stack-Overflow-in-udhcdp-TR-111-Option-125-Parsing-33cb5c52018a80238b80e89e7c7c68f0">https://tzh00203.notion.site/D-Link-DIR-822A-Stack-Overflow-in-udhcdp-TR-111-Option-125-Parsing-33cb5c52018a80238b80e89e7c7c68f0</a><br><a href="https://vuldb.com/cve/CVE-2026-86296">https://vuldb.com/cve/CVE-2026-86296</a><br><a href="https://vuldb.com/submit/906297">https://vuldb.com/submit/906297</a><br><a href="https://vuldb.com/vuln/399458">https://vuldb.com/vuln/399458</a><br><a href="https://vuldb.com/vuln/399458/cti">https://vuldb.com/vuln/399458/cti</a><br><a href="https://www.dlink.com/">https://www.dlink.com/</a> |              |             |                  |
| <a href="#">CVE-2026-79697</a> | 9,9       | Advantech WISE-6610-NB; WISE-6610-EB; WISE-6610-TB; WISE-6610-JB; WISE-6610-CB; WISE-6610-EL-NB; WISE-6610-EL-EB; WISE-6610-EL-TB; WISE-6610-EL-JB; WISE-6610-EL-CB; WISE-6610P-DEA; WISE-6610P-DNA; WISE-6610P-DTA | Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in a Command ('Command Injection') | version 1.2.4_20260821                                                                                                                                                                                                                                                             | <a href="https://uvxbywu62qm.feishu.cn/wiki/EzwXwS0vKiroHmk9rqzciP0EnMe?from=from_copylink">https://uvxbywu62qm.feishu.cn/wiki/EzwXwS0vKiroHmk9rqzciP0EnMe?from=from_copylink</a><br><a href="https://vuldb.com/cve/CVE-2026-79697">https://vuldb.com/cve/CVE-2026-79697</a><br><a href="https://vuldb.com/submit/879208">https://vuldb.com/submit/879208</a><br><a href="https://vuldb.com/vuln/399512">https://vuldb.com/vuln/399512</a><br><a href="https://vuldb.com/vuln/399512/cti">https://vuldb.com/vuln/399512/cti</a><br><a href="https://www.advantech.com/">https://www.advantech.com/</a>                                                                                       |              |             |                  |
| <a href="#">CVE-2026-86167</a> | 9,9       | Tenda HG10                                                                                                                                                                                                          | Improper Neutralization of Special Elements used in a Command ('Command Injection'); Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')         | 300001138                                                                                                                                                                                                                                                                          | <a href="https://github.com/SunnyYANGyaya/cuicuishark-sheep-fishIoT/blob/main/Tenda/HG10/command-formgponConf-fmgpon_loid.md">https://github.com/SunnyYANGyaya/cuicuishark-sheep-fishIoT/blob/main/Tenda/HG10/command-formgponConf-fmgpon_loid.md</a><br><a href="https://vuldb.com/cve/CVE-2026-86167">https://vuldb.com/cve/CVE-2026-86167</a><br><a href="https://vuldb.com/submit/895596">https://vuldb.com/submit/895596</a><br><a href="https://vuldb.com/vuln/399306">https://vuldb.com/vuln/399306</a><br><a href="https://vuldb.com/vuln/399306/cti">https://vuldb.com/vuln/399306/cti</a><br><a href="https://www.tenda.com.cn/">https://www.tenda.com.cn/</a>                     |              |             |                  |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                                                                         | Τύπος Ευπάθειας                                                                                                                                                                 | Συσκευές/Εκδόσεις που επηρεάζονται | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-86299</a> | 9,9       | Linksys RE7000                                                                                          | Improper Neutralization of Special Elements used in a Command ('Command Injection'); Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 2.0.15                             | <a href="https://github.com/limou89/somevul/blob/main/Linksys_RE7000_v2_PingTest_Command_Injection.md">https://github.com/limou89/somevul/blob/main/Linksys_RE7000_v2_PingTest_Command_Injection.md</a><br><a href="https://vuldb.com/cve/CVE-2026-86299">https://vuldb.com/cve/CVE-2026-86299</a><br><a href="https://vuldb.com/submit/906547">https://vuldb.com/submit/906547</a><br><a href="https://vuldb.com/vuln/399463">https://vuldb.com/vuln/399463</a><br><a href="https://vuldb.com/vuln/399463/ctj">https://vuldb.com/vuln/399463/ctj</a><br><a href="https://www.linksys.com/">https://www.linksys.com/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |              |             |                  |
| <a href="#">CVE-2024-11080</a> | 9,8       | The Post Grid and Gutenberg Blocks – ComboBlocks plugin for WordPress                                   | Improper Control of Generation of Code ('Code Injection')                                                                                                                       | in versions 2.2.32 to 2.3.1        | <a href="https://plugins.trac.wordpress.org/browser/post-grid/trunk/includes/blocks/form-wrap/functions.php#L116">https://plugins.trac.wordpress.org/browser/post-grid/trunk/includes/blocks/form-wrap/functions.php#L116</a><br><a href="https://plugins.trac.wordpress.org/browser/post-grid/trunk/includes/blocks/form-wrap/functions.php#L262">https://plugins.trac.wordpress.org/browser/post-grid/trunk/includes/blocks/form-wrap/functions.php#L262</a><br><a href="https://plugins.trac.wordpress.org/browser/post-grid/trunk/includes/blocks/form-wrap/functions.php#L3249">https://plugins.trac.wordpress.org/browser/post-grid/trunk/includes/blocks/form-wrap/functions.php#L3249</a><br><a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/ec8666d4-042e-4cf4-86f5-474a69d90ff6?source=cve">https://www.wordfence.com/threat-intel/vulnerabilities/id/ec8666d4-042e-4cf4-86f5-474a69d90ff6?source=cve</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | none         | yes         | total            |
| <a href="#">CVE-2026-10196</a> | 9,8       | The Mail Mint – Email Marketing, Newsletter, Email Automation & WooCommerce Emails plugin for WordPress | Deserialization of Untrusted Data                                                                                                                                               | up to, and including, 1.31.0       | <a href="https://plugins.trac.wordpress.org/browser/mail-mint/tags/1.21.0/app/API/Actions/Frontend/FormAction.php#L59">https://plugins.trac.wordpress.org/browser/mail-mint/tags/1.21.0/app/API/Actions/Frontend/FormAction.php#L59</a><br><a href="https://plugins.trac.wordpress.org/browser/mail-mint/tags/1.21.0/app/Database/models/ContactModel.php#L460">https://plugins.trac.wordpress.org/browser/mail-mint/tags/1.21.0/app/Database/models/ContactModel.php#L460</a><br><a href="https://plugins.trac.wordpress.org/browser/mail-mint/tags/1.21.0/vendor/posthog/posthog-php/lib/Consumer/ForkCurl.php#L96">https://plugins.trac.wordpress.org/browser/mail-mint/tags/1.21.0/vendor/posthog/posthog-php/lib/Consumer/ForkCurl.php#L96</a><br><a href="https://plugins.trac.wordpress.org/browser/mail-mint/trunk/app/API/Actions/Frontend/FormAction.php#L59">https://plugins.trac.wordpress.org/browser/mail-mint/trunk/app/API/Actions/Frontend/FormAction.php#L59</a><br><a href="https://plugins.trac.wordpress.org/browser/mail-mint/trunk/app/Database/models/ContactModel.php#L460">https://plugins.trac.wordpress.org/browser/mail-mint/trunk/app/Database/models/ContactModel.php#L460</a><br><a href="https://plugins.trac.wordpress.org/browser/mail-mint/trunk/vendor/posthog/posthog-php/lib/Consumer/ForkCurl.php#L96">https://plugins.trac.wordpress.org/browser/mail-mint/trunk/vendor/posthog/posthog-php/lib/Consumer/ForkCurl.php#L96</a> | none         | yes         | total            |
| <a href="#">CVE-2026-13447</a> | 9,8       | The Mstore Api plugin for WordPress                                                                     | Improper Authentication                                                                                                                                                         | up to, and including, 4.20.0       | <a href="https://plugins.trac.wordpress.org/browser/mstore-api/tags/4.18.4/controllers/flutter-user.php#L829">https://plugins.trac.wordpress.org/browser/mstore-api/tags/4.18.4/controllers/flutter-user.php#L829</a><br><a href="https://plugins.trac.wordpress.org/browser/mstore-api/tags/4.18.4/controllers/flutter-user.php#L940">https://plugins.trac.wordpress.org/browser/mstore-api/tags/4.18.4/controllers/flutter-user.php#L940</a><br><a href="https://plugins.trac.wordpress.org/browser/mstore-api/tags/4.18.4/controllers/helpers/firebase-phone-auth-helper.php#L5">https://plugins.trac.wordpress.org/browser/mstore-api/tags/4.18.4/controllers/helpers/firebase-phone-auth-helper.php#L5</a><br><a href="https://plugins.trac.wordpress.org/browser/mstore-api/trunk/controllers/flutter-user.php#L829">https://plugins.trac.wordpress.org/browser/mstore-api/trunk/controllers/flutter-user.php#L829</a><br><a href="https://plugins.trac.wordpress.org/browser/mstore-api/trunk/controllers/flutter-user.php#L940">https://plugins.trac.wordpress.org/browser/mstore-api/trunk/controllers/flutter-user.php#L940</a><br><a href="https://plugins.trac.wordpress.org/browser/mstore-api/trunk/controllers/helpers/firebase-phone-auth-helper.php#L5">https://plugins.trac.wordpress.org/browser/mstore-api/trunk/controllers/helpers/firebase-phone-auth-helper.php#L5</a>                                                                         | none         | yes         | total            |
| <a href="#">CVE-2026-16310</a> | 9,8       | The MemberDash plugin for WordPress;                                                                    | Authorization Bypass Through User-Controlled Key                                                                                                                                | up to, and including, 1.8.5        | <a href="https://www.memberdashwp.com">https://www.memberdashwp.com</a><br><a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/222e0f27-f269-4751-9544-1a6cb03ab3a7?source=cve">https://www.wordfence.com/threat-intel/vulnerabilities/id/222e0f27-f269-4751-9544-1a6cb03ab3a7?source=cve</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | none         | yes         | total            |
| <a href="#">CVE-2026-18922</a> | 9,8       | 389 Directory Server                                                                                    | Improper Authentication                                                                                                                                                         |                                    | <a href="https://access.redhat.com/errata/RHSA-2026:64771">https://access.redhat.com/errata/RHSA-2026:64771</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64776">https://access.redhat.com/errata/RHSA-2026:64776</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64778">https://access.redhat.com/errata/RHSA-2026:64778</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64779">https://access.redhat.com/errata/RHSA-2026:64779</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64781">https://access.redhat.com/errata/RHSA-2026:64781</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64783">https://access.redhat.com/errata/RHSA-2026:64783</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |              |             |                  |
| <a href="#">CVE-2026-58240</a> | 9,8       | SAP NetWeaver (Message Server)                                                                          | Use of Single-factor Authentication                                                                                                                                             | KERNEL 9.16; 9.18; 9.19; 9.20      | <a href="https://me.sap.com/notes/3759472">https://me.sap.com/notes/3759472</a><br><a href="https://url.sap/sapsecuritypatchday">https://url.sap/sapsecuritypatchday</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |              |             |                  |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                                                            | Τύπος Ευπάθειας                                           | Συσκευές/Εκδόσεις που επηρεάζονται                | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-75816</a> | 9,8       | The Frontend Admin by DynamiApps plugin for WordPress                                      | Improper Authentication                                   | up to, and including, 3.29.12.                    | <a href="https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/fields/user/class-user-email.php#L127">https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/fields/user/class-user-email.php#L127</a><br><a href="https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/actions/post.php#L1001">https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/actions/post.php#L1001</a><br><a href="https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/actions/post.php#L1224">https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/actions/post.php#L1224</a><br><a href="https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/classes/display.php#L26">https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/classes/display.php#L26</a><br><a href="https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/classes/submit.php#L125">https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/classes/submit.php#L125</a><br><a href="https://plugins.trac.wordpress.org/changeset/3664865/acf-frontend-form-element">https://plugins.trac.wordpress.org/changeset/3664865/acf-frontend-form-element</a> | none         | yes         | total            |
| <a href="#">CVE-2026-76578</a> | 9,8       | FreelPA                                                                                    | Missing Authentication for Critical Function              |                                                   | <a href="https://access.redhat.com/security/cve/CVE-2026-76578">https://access.redhat.com/security/cve/CVE-2026-76578</a><br><a href="https://bugzilla.redhat.com/show_bug.cgi?id=2519522">https://bugzilla.redhat.com/show_bug.cgi?id=2519522</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |              |             |                  |
| <a href="#">CVE-2026-78362</a> | 9,8       | The SEO Flow by LupsOnline WordPress plugin                                                | Improper Privilege Management                             | before 3.0.3                                      | <a href="https://wpscan.com/vulnerability/0833424b-1231-4a48-be90-13fe4edc60c9/">https://wpscan.com/vulnerability/0833424b-1231-4a48-be90-13fe4edc60c9/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | none         | yes         | total            |
| <a href="#">CVE-2026-7861</a>  | 9,8       | Next4Biz Information Technologies Inc                                                      | Deserialization of Untrusted Data                         | through 07092026.                                 | <a href="https://siberquvenlik.gov.tr/quvenlik-bildirimleri/detay/tr-26-1027">https://siberquvenlik.gov.tr/quvenlik-bildirimleri/detay/tr-26-1027</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |              |             |                  |
| <a href="#">CVE-2026-83627</a> | 9,8       | The Hummingbird – Speed Optimization, Caching, Minify, Compress & CDN plugin for WordPress | Improper Control of Generation of Code ('Code Injection') | up to, and including, 3.21.0                      | <a href="https://plugins.trac.wordpress.org/browser/hummingbird-performance/trunk/core/modules/class-page-cache.php#L1973">https://plugins.trac.wordpress.org/browser/hummingbird-performance/trunk/core/modules/class-page-cache.php#L1973</a><br><a href="https://plugins.trac.wordpress.org/browser/hummingbird-performance/trunk/core/modules/class-page-cache.php#L1982">https://plugins.trac.wordpress.org/browser/hummingbird-performance/trunk/core/modules/class-page-cache.php#L1982</a><br><a href="https://plugins.trac.wordpress.org/browser/hummingbird-performance/trunk/core/modules/class-page-cache.php#L749">https://plugins.trac.wordpress.org/browser/hummingbird-performance/trunk/core/modules/class-page-cache.php#L749</a><br><a href="https://plugins.trac.wordpress.org/browser/hummingbird-performance/trunk/core/modules/class-page-cache.php#L752">https://plugins.trac.wordpress.org/browser/hummingbird-performance/trunk/core/modules/class-page-cache.php#L752</a><br><a href="https://plugins.trac.wordpress.org/changeset/3675836/hummingbird-performance/trunk/core/modules/class-page-cache.php">https://plugins.trac.wordpress.org/changeset/3675836/hummingbird-performance/trunk/core/modules/class-page-cache.php</a><br><a href="https://plugins.trac.wordpress.org/changeset?old_path=%2Fhummingbird-performance/tags/3.20.0&amp;new_path=%2Fhummingbird-performance/tags/3.21.2">https://plugins.trac.wordpress.org/changeset?old_path=%2Fhummingbird-performance/tags/3.20.0&amp;new_path=%2Fhummingbird-performance/tags/3.21.2</a>       | none         | yes         | total            |
| <a href="#">CVE-2026-86478</a> | 9,8       | In JetBrains YouTrack                                                                      | Authentication Bypass by Spoofing                         | before 2025.3.161254, 2026.1.14042                | <a href="https://www.jetbrains.com/privacy-security/issues-fixed/">https://www.jetbrains.com/privacy-security/issues-fixed/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |              |             |                  |
| <a href="#">CVE-2026-86480</a> | 9,8       | In JetBrains Hub                                                                           | Missing Authentication for Critical Function              | before 2026.2.52442                               | <a href="https://www.jetbrains.com/privacy-security/issues-fixed/">https://www.jetbrains.com/privacy-security/issues-fixed/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |              |             |                  |
| <a href="#">CVE-2026-86543</a> | 9,8       | knowns versions                                                                            | Missing Authentication for Critical Function              | versions before 0.30.0                            | <a href="https://github.com/knowns-dev/knowns/blob/v0.29.1/internal/cli/browser.go#L193-L200">https://github.com/knowns-dev/knowns/blob/v0.29.1/internal/cli/browser.go#L193-L200</a><br><a href="https://github.com/knowns-dev/knowns/blob/v0.29.1/internal/server/auth.go#L80-L86">https://github.com/knowns-dev/knowns/blob/v0.29.1/internal/server/auth.go#L80-L86</a><br><a href="https://github.com/knowns-dev/knowns/blob/v0.29.1/internal/server/routes/tunnel.go#L26-L38">https://github.com/knowns-dev/knowns/blob/v0.29.1/internal/server/routes/tunnel.go#L26-L38</a><br><a href="https://github.com/knowns-dev/knowns/commit/878a02cb7cc14f0a592fd7da7a520af3cac500fb">https://github.com/knowns-dev/knowns/commit/878a02cb7cc14f0a592fd7da7a520af3cac500fb</a><br><a href="https://github.com/knowns-dev/knowns/releases/tag/v0.30.0">https://github.com/knowns-dev/knowns/releases/tag/v0.30.0</a><br><a href="https://github.com/knowns-dev/knowns/security/advisories/GHSA-fc85-99vc-9c75">https://github.com/knowns-dev/knowns/security/advisories/GHSA-fc85-99vc-9c75</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |              |             |                  |
| <a href="#">CVE-2026-76969</a> | 9,4       | @sap/cds-mtxs NPM library                                                                  | Insufficiently Protected Credentials                      | @sap/cds-mtxs <=1.18.3; <=2.7.6; <=3.9.6; <=4.0.2 | <a href="https://me.sap.com/notes/3798315">https://me.sap.com/notes/3798315</a><br><a href="https://url.sap.sapsecuritypatchday">https://url.sap.sapsecuritypatchday</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |              |             |                  |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                           | Τύπος Ευπάθειας                                                                      | Συσκευές/Εκδόσεις που επηρεάζονται | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|-----------------------------------------------------------|--------------------------------------------------------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-66768</a> | 9,0       | SAP NetWeaver (SAP GUI for Java)                          | Reliance on Untrusted Inputs in a Security Decision                                  | BC-FES-JAV 8.10                    | <a href="https://me.sap.com/notes/3781729">https://me.sap.com/notes/3781729</a><br><a href="https://url.sap/sapsecuritypatchday">https://url.sap/sapsecuritypatchday</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |              |             |                  |
| <a href="#">CVE-2026-48019</a> | 8,9       | Laravel                                                   | Improper Neutralization of CRLF Sequences ('CRLF Injection')                         | >= 13.0.0, < 13.10.0; < 12.60.0    | <a href="https://github.com/laravel/framework/commit/96e9a663db657cf37ef26cd794fda8ff60eaa451">https://github.com/laravel/framework/commit/96e9a663db657cf37ef26cd794fda8ff60eaa451</a><br><a href="https://github.com/laravel/framework/commit/f336ba79e744257f84ebf0d096b0ebc62e8e1a4d">https://github.com/laravel/framework/commit/f336ba79e744257f84ebf0d096b0ebc62e8e1a4d</a><br><a href="https://github.com/laravel/framework/pull/60151">https://github.com/laravel/framework/pull/60151</a><br><a href="https://github.com/laravel/framework/releases/tag/v12.60.0">https://github.com/laravel/framework/releases/tag/v12.60.0</a><br><a href="https://github.com/laravel/framework/releases/tag/v13.10.0">https://github.com/laravel/framework/releases/tag/v13.10.0</a><br><a href="https://github.com/laravel/framework/security/advisories/GHSA-5vg9-5847-vvmq">https://github.com/laravel/framework/security/advisories/GHSA-5vg9-5847-vvmq</a>                                                                                                                                                                                 |              |             |                  |
| <a href="#">CVE-2025-9049</a>  | 8,8       | The Nokri – Job Board WordPress Theme theme for WordPress | Missing Authorization                                                                | up to, and including, 1.6.4.       | <a href="https://theforest.net/item/nokri-job-board-wordpress-theme/22677241#item-description_nokri-theme-change-logs">https://theforest.net/item/nokri-job-board-wordpress-theme/22677241#item-description_nokri-theme-change-logs</a><br><a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/e079e886-70a5-4188-ad99-96fc37651ed0?source=cve">https://www.wordfence.com/threat-intel/vulnerabilities/id/e079e886-70a5-4188-ad99-96fc37651ed0?source=cve</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | none         | no          | total            |
| <a href="#">CVE-2026-18480</a> | 8,8       | The SureCart WordPress plugin                             | Improper Privilege Management                                                        | before 4.6.3                       | <a href="https://wpscan.com/vulnerability/88839ada-9c59-44cb-96e6-3548e5a59b9f/">https://wpscan.com/vulnerability/88839ada-9c59-44cb-96e6-3548e5a59b9f/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | none         | no          | total            |
| <a href="#">CVE-2026-19633</a> | 8,8       | PostgreSQL Anonymizer                                     | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 3.1.4 and later                    | <a href="https://gitlab.com/dalibo/postgresql_anonymizer/-/issues/665">https://gitlab.com/dalibo/postgresql_anonymizer/-/issues/665</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |              |             |                  |
| <a href="#">CVE-2026-77393</a> | 8,8       | Ignition                                                  | Incorrect Default Permissions                                                        | 8.1.53 and earlier                 | <a href="https://github.com/cisaqov/CSAF/blob/develop/csaf_files/OT/w/hitel/2026/icsa-26-246-06.json">https://github.com/cisaqov/CSAF/blob/develop/csaf_files/OT/w/hitel/2026/icsa-26-246-06.json</a><br><a href="https://security.inductiveautomation.com/?tcuUId=34477620-731d-4b70-b22b-9450f9a659a3">https://security.inductiveautomation.com/?tcuUId=34477620-731d-4b70-b22b-9450f9a659a3</a><br><a href="https://www.cisa.gov/news-events/ics-advisories/icsa-26-246-06">https://www.cisa.gov/news-events/ics-advisories/icsa-26-246-06</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | none         | no          | total            |
| <a href="#">CVE-2026-77826</a> | 8,8       | The RegistrationMagic WordPress plugin                    | Improper Authentication                                                              | before 6.0.9.9                     | <a href="https://wpscan.com/vulnerability/b79a83e8-d7b0-4aa8-b2ba-37a7eecd437b/">https://wpscan.com/vulnerability/b79a83e8-d7b0-4aa8-b2ba-37a7eecd437b/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | none         | no          | total            |
| <a href="#">CVE-2026-82712</a> | 8,8       | Tycon Systems TPDIN-Monitor-WEB3                          | Cross-Site Request Forgery (CSRF)                                                    | versions 2.2.9 and prior           | <a href="https://firm.tyconsystems.com/tpdin-monitor-web3-v2/TPDIN-MONITOR-WEB3-V2_v2.4.2.tfw">https://firm.tyconsystems.com/tpdin-monitor-web3-v2/TPDIN-MONITOR-WEB3-V2_v2.4.2.tfw</a><br><a href="https://firm.tyconsystems.com/tpdin-monitor-web3-v2/TPDIN-MONITOR-WEB3-V2_v2.4.2T.hex">https://firm.tyconsystems.com/tpdin-monitor-web3-v2/TPDIN-MONITOR-WEB3-V2_v2.4.2T.hex</a><br><a href="https://github.com/cisaqov/CSAF/blob/develop/csaf_files/OT/w/hitel/2026/icsa-26-246-08.json">https://github.com/cisaqov/CSAF/blob/develop/csaf_files/OT/w/hitel/2026/icsa-26-246-08.json</a><br><a href="https://www.cisa.gov/news-events/ics-advisories/icsa-26-246-08">https://www.cisa.gov/news-events/ics-advisories/icsa-26-246-08</a>                                                                                                                                                                                                                                                                                                                                                                                                 | none         | no          | total            |
| <a href="#">CVE-2026-86169</a> | 8,8       | Axolotl                                                   | Inclusion of Functionality from Untrusted Control Sphere                             | through 0.18.0                     | <a href="https://github.com/axolotl-ai-cloud/axolotl">https://github.com/axolotl-ai-cloud/axolotl</a><br><a href="https://github.com/axolotl-ai-cloud/axolotl/blob/v0.18.0/src/axolotl/loaders/patch_manager.py#L794-L806">https://github.com/axolotl-ai-cloud/axolotl/blob/v0.18.0/src/axolotl/loaders/patch_manager.py#L794-L806</a><br><a href="https://github.com/axolotl-ai-cloud/axolotl/blob/v0.18.0/src/axolotl/monkeypatch/multipack.py#L86-L96">https://github.com/axolotl-ai-cloud/axolotl/blob/v0.18.0/src/axolotl/monkeypatch/multipack.py#L86-L96</a><br><a href="https://github.com/axolotl-ai-cloud/axolotl/commit/b62d60b101eea7f32532ee3c0b17c2f2430a9262">https://github.com/axolotl-ai-cloud/axolotl/commit/b62d60b101eea7f32532ee3c0b17c2f2430a9262</a><br><a href="https://github.com/axolotl-ai-cloud/axolotl/pull/3858">https://github.com/axolotl-ai-cloud/axolotl/pull/3858</a><br><a href="https://www.vulncheck.com/advisories/axolotl-through-0.18.0-remote-code-execution-via-multipack-patching">https://www.vulncheck.com/advisories/axolotl-through-0.18.0-remote-code-execution-via-multipack-patching</a> |              |             |                  |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                                                                                                                                                                                                                                                         | Τύπος Ευπάθειας                                                                            | Συσκευές/Εκδόσεις που επηρεάζονται                                                                                                       | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-86177</a> | 8,8       | Pterodactyl Panel                                                                                                                                                                                                                                                                       | Missing Authorization                                                                      | before 1.14.1                                                                                                                            | <a href="https://github.com/geo-chen/oss/blob/main/panel.md">https://github.com/geo-chen/oss/blob/main/panel.md</a><br><a href="https://github.com/pterodactyl/panel">https://github.com/pterodactyl/panel</a><br><a href="https://github.com/pterodactyl/panel/blob/v1.14.0/app/Http/Requests/Api/Client/Servers/Schedules/StoreTaskRequest.php#L10-L25">https://github.com/pterodactyl/panel/blob/v1.14.0/app/Http/Requests/Api/Client/Servers/Schedules/StoreTaskRequest.php#L10-L25</a><br><a href="https://github.com/pterodactyl/panel/blob/v1.14.0/app/Jobs/Schedule/RunTaskJob.php#L60-L75">https://github.com/pterodactyl/panel/blob/v1.14.0/app/Jobs/Schedule/RunTaskJob.php#L60-L75</a><br><a href="https://github.com/pterodactyl/panel/commit/913b354aff43ff04f4ce95357ed68a675a1dd0fa6">https://github.com/pterodactyl/panel/commit/913b354aff43ff04f4ce95357ed68a675a1dd0fa6</a><br><a href="https://github.com/pterodactyl/panel/releases/tag/v1.14.1">https://github.com/pterodactyl/panel/releases/tag/v1.14.1</a> |              |             |                  |
| <a href="#">CVE-2026-86404</a> | 8,8       | Red Hat JBoss Enterprise Application Platform 7.4 ELS on RHEL 7; Red Hat AMQ Broker 7; Red Hat build of Apache Camel 4 for Quarkus 3; Red Hat build of Apache Camel for Spring Boot 4; Red Hat JBoss Enterprise Application Platform 7; Red Hat JBoss Enterprise Application Platform 8 | Deserialization of Untrusted Data                                                          |                                                                                                                                          | <a href="https://access.redhat.com/errata/RHSA-2026-53644">https://access.redhat.com/errata/RHSA-2026-53644</a><br><a href="https://access.redhat.com/security/cve/CVE-2026-86404">https://access.redhat.com/security/cve/CVE-2026-86404</a><br><a href="https://bugzilla.redhat.com/show_bug.cgi?id=2477930">https://bugzilla.redhat.com/show_bug.cgi?id=2477930</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |              |             |                  |
| <a href="#">CVE-2026-86427</a> | 8,8       | LibreNMS                                                                                                                                                                                                                                                                                | Improper Neutralization of Special Elements used in a Command ('Command Injection')        | before 26.8.0                                                                                                                            | <a href="https://github.com/librenms/librenms/security/advisories/GHSA-3hvv-wxpw-cx83">https://github.com/librenms/librenms/security/advisories/GHSA-3hvv-wxpw-cx83</a><br><a href="https://www.vulncheck.com/advisories/librenms-before-26.8.0-argument-injection-via-graph-title">https://www.vulncheck.com/advisories/librenms-before-26.8.0-argument-injection-via-graph-title</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |              |             |                  |
| <a href="#">CVE-2026-0799</a>  | 8,7       | In BPF instructions that                                                                                                                                                                                                                                                                | Out-of-bounds Read; Improper Validation of Array Index; Out-of-bounds Write                | prior to 1.10.7                                                                                                                          | <a href="https://github.com/the-tcpdump-group/libpcap/commit/48e8960a7108e9e828f9d7bdc7e97bda6841aec7">https://github.com/the-tcpdump-group/libpcap/commit/48e8960a7108e9e828f9d7bdc7e97bda6841aec7</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |              |             |                  |
| <a href="#">CVE-2026-86123</a> | 8,7       | SQL Chat                                                                                                                                                                                                                                                                                | Server-Side Request Forgery (SSRF)                                                         | 665af875413affadfeeff81794f1d7758782bc2 and earlier                                                                                      | <a href="https://github.com/sqlchat/sqlchat">https://github.com/sqlchat/sqlchat</a><br><a href="https://github.com/sqlchat/sqlchat/blob/665af875413affadfeeff81794f1d7758782bc2/src/pages/api/connection/execute.ts">https://github.com/sqlchat/sqlchat/blob/665af875413affadfeeff81794f1d7758782bc2/src/pages/api/connection/execute.ts</a><br><a href="https://github.com/sqlchat/sqlchat/blob/665af875413affadfeeff81794f1d7758782bc2/src/pages/api/connection/test.ts">https://github.com/sqlchat/sqlchat/blob/665af875413affadfeeff81794f1d7758782bc2/src/pages/api/connection/test.ts</a><br><a href="https://github.com/sqlchat/sqlchat/issues/189">https://github.com/sqlchat/sqlchat/issues/189</a><br><a href="https://www.vulncheck.com/advisories/sql-chat-unauthenticated-database-connection-proxy-in-the-api-connection-endpoints">https://www.vulncheck.com/advisories/sql-chat-unauthenticated-database-connection-proxy-in-the-api-connection-endpoints</a>                                                        |              |             |                  |
| <a href="#">CVE-2026-82304</a> | 8,6       | The Music Store WordPress plugin                                                                                                                                                                                                                                                        | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')       | before 1.4.5                                                                                                                             | <a href="https://wpscan.com/vulnerability/0a4d2ffc-a437-430e-a760-d8d7fb388f0c/">https://wpscan.com/vulnerability/0a4d2ffc-a437-430e-a760-d8d7fb388f0c/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | none         | yes         | partial          |
| <a href="#">CVE-2026-76958</a> | 8,5       | SAP Integration Suite                                                                                                                                                                                                                                                                   | Improper Restriction of XML External Entity Reference                                      | Cloud Integration - Trading Partner Management V2 2.9.2; B2B Integration Factory - Cloud Integration - Trading Partner Management 1.10.0 | <a href="https://me.sap.com/notes/3792978">https://me.sap.com/notes/3792978</a><br><a href="https://url.sap.com/sapsecuritypatchday">https://url.sap.com/sapsecuritypatchday</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |              |             |                  |
| <a href="#">CVE-2026-19843</a> | 8,4       | 389-ds-base                                                                                                                                                                                                                                                                             | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |                                                                                                                                          | <a href="https://access.redhat.com/errata/RHSA-2026-64768">https://access.redhat.com/errata/RHSA-2026-64768</a><br><a href="https://access.redhat.com/errata/RHSA-2026-64769">https://access.redhat.com/errata/RHSA-2026-64769</a><br><a href="https://access.redhat.com/errata/RHSA-2026-64779">https://access.redhat.com/errata/RHSA-2026-64779</a><br><a href="https://access.redhat.com/errata/RHSA-2026-64782">https://access.redhat.com/errata/RHSA-2026-64782</a><br><a href="https://access.redhat.com/errata/RHSA-2026-64792">https://access.redhat.com/errata/RHSA-2026-64792</a><br><a href="https://access.redhat.com/security/cve/CVE-2026-19843">https://access.redhat.com/security/cve/CVE-2026-19843</a>                                                                                                                                                                                                                                                                                                             |              |             |                  |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                             | Τύπος Ευπάθειας                                                                      | Συσκευές/Εκδόσεις που επηρεάζονται                                                                                                                                                                                                                                                                                                                                                                                                      | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|-------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-20501</a> | 8,4       | In vdec                                                     | Heap-based Buffer Overflow                                                           | MT2718; MT6580; MT6739; MT6761; MT6765; MT6768; MT6769; MT6779; MT6781; MT6785; MT6789; MT6833; MT6835; MT6853; MT6855; MT6858; MT6873; MT6877; MT6878; MT6879; MT6881; MT6883; MT6885; MT6886; MT6889; MT6893; MT6895; MT6897; MT6899; MT6983; MT6985; MT6989; MT6991; MT6993; MT8126; MT8171; MT8186; MT8188; MT8189; MT8195; MT8196; MT8367; MT8391; MT8395; MT8668; MT8676; MT8678; MT8696; MT8781; MT8788E; MT8792; MT8799; MT8910 | <a href="https://www.mediatek.com/product-security-bulletin/September-2026">https://www.mediatek.com/product-security-bulletin/September-2026</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | none         | no          | total            |
| <a href="#">CVE-2026-86502</a> | 8,4       | In JetBrains IntelliJ IDEA                                  | Missing Authentication for Critical Function                                         | before 2026.2.2                                                                                                                                                                                                                                                                                                                                                                                                                         | <a href="https://www.jetbrains.com/privacy-security/issues-fixed/">https://www.jetbrains.com/privacy-security/issues-fixed/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |              |             |                  |
| <a href="#">CVE-2026-84934</a> | 8,0       | The JCH Optimize WordPress plugin                           | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | before 6.0.1                                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="https://wpscan.com/vulnerability/d808ad17-d20e-4ee5-94f3-935c10cde772/">https://wpscan.com/vulnerability/d808ad17-d20e-4ee5-94f3-935c10cde772/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | none         | no          | total            |
| <a href="#">CVE-2026-84935</a> | 8,0       | The HT Menu WordPress plugin                                | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | before 1.2.7                                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="https://wpscan.com/vulnerability/10aeb456-764d-4f4d-a2c9-e357474d59c7/">https://wpscan.com/vulnerability/10aeb456-764d-4f4d-a2c9-e357474d59c7/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | none         | no          | total            |
| <a href="#">CVE-2026-76967</a> | 7,8       | SAP NetWeaver Business Client                               | Deserialization of Untrusted Data                                                    | BC-WD-CLT-BUS 8.00; 8.10                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="https://me.sap.com/notes/3784138">https://me.sap.com/notes/3784138</a><br><a href="https://url.sap.sapsecuritypatchday">https://url.sap.sapsecuritypatchday</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |              |             |                  |
| <a href="#">CVE-2026-86095</a> | 7,8       | Unidata netcdf-c                                            | Out-of-bounds Write                                                                  | through 4.10.1                                                                                                                                                                                                                                                                                                                                                                                                                          | <a href="https://github.com/Unidata/netcdf-c">https://github.com/Unidata/netcdf-c</a><br><a href="https://github.com/Unidata/netcdf-c/blob/v4.10.1/libhdf5/hdf5attr.c">https://github.com/Unidata/netcdf-c/blob/v4.10.1/libhdf5/hdf5attr.c</a><br><a href="https://www.vulncheck.com/advisories/unidata-netcdf-c-through-4.10.1-out-of-bounds-write-via-oversized-hdf5-attribute-name">https://www.vulncheck.com/advisories/unidata-netcdf-c-through-4.10.1-out-of-bounds-write-via-oversized-hdf5-attribute-name</a>                                                                                                                                                                                                                                                                                      |              |             |                  |
| <a href="#">CVE-2026-86313</a> | 7,8       | Samsung Opensource Walrus                                   | Out-of-bounds Write                                                                  | af80e665ea49d9003695a66502f841ed1d8397e7                                                                                                                                                                                                                                                                                                                                                                                                | <a href="https://github.com/Samsung/walrus/pull/482">https://github.com/Samsung/walrus/pull/482</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |              |             |                  |
| <a href="#">CVE-2026-66767</a> | 7,7       | SAP NetWeaver Application Server for ABAP and ABAP Platform | Integer Underflow (Wrap or Wraparound)                                               | KRNL64NUC 7.22; 7.22EXT; KRNL64UC 7.22; 7.53; 8.04; KERNEL 7.22; 7.54; 7.77; 7.93; 9.16; 9.18; 9.19; 9.20                                                                                                                                                                                                                                                                                                                               | <a href="https://me.sap.com/notes/3757002">https://me.sap.com/notes/3757002</a><br><a href="https://url.sap.sapsecuritypatchday">https://url.sap.sapsecuritypatchday</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |              |             |                  |
| <a href="#">CVE-2022-51009</a> | 7,5       | PocketMine-MP                                               | Uncaught Exception                                                                   | before 4.7.2                                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="https://github.com/pmmp/PocketMine-MP/commit/c9626c610b8f6810c8c987559c9197b2a291f0bb">https://github.com/pmmp/PocketMine-MP/commit/c9626c610b8f6810c8c987559c9197b2a291f0bb</a><br><a href="https://github.com/pmmp/PocketMine-MP/security/advisories/GHSA-8cwq-4cmf-px73">https://github.com/pmmp/PocketMine-MP/security/advisories/GHSA-8cwq-4cmf-px73</a><br><a href="https://www.vulncheck.com/advisories/pocketmine-mp-before-4.7.2-denial-of-service-via-skin-geometry">https://www.vulncheck.com/advisories/pocketmine-mp-before-4.7.2-denial-of-service-via-skin-geometry</a>                                                                                                                                                                                                            |              |             |                  |
| <a href="#">CVE-2022-51017</a> | 7,5       | PocketMine-MP versions                                      | Improper Input Validation                                                            | versions before 3.26.5 and 4.0.5                                                                                                                                                                                                                                                                                                                                                                                                        | <a href="https://github.com/pmmp/PocketMine-MP/commit/6492cac5c10f9fa8443ceddd2191a7b65b73f601">https://github.com/pmmp/PocketMine-MP/commit/6492cac5c10f9fa8443ceddd2191a7b65b73f601</a><br><a href="https://github.com/pmmp/PocketMine-MP/commit/958a9dbf0fe3131ab60319c5a939f5dfbfe5dfbb">https://github.com/pmmp/PocketMine-MP/commit/958a9dbf0fe3131ab60319c5a939f5dfbfe5dfbb</a><br><a href="https://github.com/pmmp/PocketMine-MP/security/advisories/GHSA-c6fq-99pr-25m9">https://github.com/pmmp/PocketMine-MP/security/advisories/GHSA-c6fq-99pr-25m9</a><br><a href="https://www.vulncheck.com/advisories/pocketmine-mp-before-3.26.5-and-4.0.5-denial-of-service-via-skin-data">https://www.vulncheck.com/advisories/pocketmine-mp-before-3.26.5-and-4.0.5-denial-of-service-via-skin-data</a> |              |             |                  |
| <a href="#">CVE-2026-14296</a> | 7,5       | nRF54H20                                                    | Improper Verification of Cryptographic Signature                                     | 3.2; 3.3                                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="https://docs.nordicsemi.com/r/bundle/struct_sa/page/struct_sa.html">https://docs.nordicsemi.com/r/bundle/struct_sa/page/struct_sa.html</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |              |             |                  |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                                   | Τύπος Ευπάθειας                                                                            | Συσκευές/Εκδόσεις που επηρεάζονται | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-18056</a> | 7,5       | The HivePress Authentication plugin for WordPress                 | Improper Authentication                                                                    | up to, and including, 1.1.4.       | <a href="https://developers.facebook.com/docs/facebook-login/guides/advanced/manual-flow/#confirm">https://developers.facebook.com/docs/facebook-login/guides/advanced/manual-flow/#confirm</a><br><a href="https://github.com/hivepress/hivepress-authentication/commit/f97d9109002905cf57597d15c535d1155dc64657">https://github.com/hivepress/hivepress-authentication/commit/f97d9109002905cf57597d15c535d1155dc64657</a><br><a href="https://plugins.trac.wordpress.org/browser/hivepress-authentication/tags/1.1.4/includes/components/class-facebook-authentication.php#L59">https://plugins.trac.wordpress.org/browser/hivepress-authentication/tags/1.1.4/includes/components/class-facebook-authentication.php#L59</a><br><a href="https://plugins.trac.wordpress.org/browser/hivepress-authentication/tags/1.1.4/includes/controllers/class-authentication.php#L84">https://plugins.trac.wordpress.org/browser/hivepress-authentication/tags/1.1.4/includes/controllers/class-authentication.php#L84</a><br><a href="https://plugins.trac.wordpress.org/changeset/3664231/hivepress-authentication">https://plugins.trac.wordpress.org/changeset/3664231/hivepress-authentication</a><br><a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/c0ba6392-e6f7-479a-8b9b-9cea4b140c71?source=cve">https://www.wordfence.com/threat-intel/vulnerabilities/id/c0ba6392-e6f7-479a-8b9b-9cea4b140c71?source=cve</a> | none         | no          | total            |
| <a href="#">CVE-2026-18355</a> | 7,5       | SASL I/O layer of 389 Directory Server (389-ds-base).             | Integer Underflow (Wrap or Wraparound)                                                     | > 0)                               | <a href="https://access.redhat.com/errata/RHSA-2026:64771">https://access.redhat.com/errata/RHSA-2026:64771</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64776">https://access.redhat.com/errata/RHSA-2026:64776</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64778">https://access.redhat.com/errata/RHSA-2026:64778</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64779">https://access.redhat.com/errata/RHSA-2026:64779</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64781">https://access.redhat.com/errata/RHSA-2026:64781</a><br><a href="https://access.redhat.com/errata/RHSA-2026:64783">https://access.redhat.com/errata/RHSA-2026:64783</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |              |             |                  |
| <a href="#">CVE-2026-19858</a> | 7,5       | The JetFormBuilder — Dynamic Blocks Form Builder WordPress plugin | Exposure of Sensitive Information to an Unauthorized Actor                                 | before 3.6.5.2                     | <a href="https://wpscan.com/vulnerability/a9d091f3-6887-4f26-a736-ba26a81d2b32/">https://wpscan.com/vulnerability/a9d091f3-6887-4f26-a736-ba26a81d2b32/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | none         | yes         | partial          |
| <a href="#">CVE-2026-84219</a> | 7,5       | The Kirki WordPress plugin                                        | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')       | before 6.3.0                       | <a href="https://wpscan.com/vulnerability/e95bd1e3-6f61-423f-add6-519e1ca7bf66/">https://wpscan.com/vulnerability/e95bd1e3-6f61-423f-add6-519e1ca7bf66/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | none         | no          | total            |
| <a href="#">CVE-2026-86250</a> | 7,5       | h3 versions                                                       | Uncontrolled Resource Consumption                                                          | versions before 2.0.1-rc.18        | <a href="https://github.com/h3js/h3/security/advisories/GHSA-q5pr-72pg-83v3">https://github.com/h3js/h3/security/advisories/GHSA-q5pr-72pg-83v3</a><br><a href="https://www.vulncheck.com/advisories/h3-before-2.0.1-rc.18-denial-of-service-via-unbounded-chunked-cookie">https://www.vulncheck.com/advisories/h3-before-2.0.1-rc.18-denial-of-service-via-unbounded-chunked-cookie</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |              |             |                  |
| <a href="#">CVE-2026-86259</a> | 7,5       | OpenMAIC                                                          | Missing Authentication for Critical Function; Server-Side Request Forgery (SSRF)           | before 1.0.1                       | <a href="https://github.com/THU-MAIC/OpenMAIC">https://github.com/THU-MAIC/OpenMAIC</a><br><a href="https://github.com/THU-MAIC/OpenMAIC/blob/v1.0.0/app/api/generate/image/route.ts#L73-L78">https://github.com/THU-MAIC/OpenMAIC/blob/v1.0.0/app/api/generate/image/route.ts#L73-L78</a><br><a href="https://github.com/THU-MAIC/OpenMAIC/blob/v1.0.0/middleware.ts#L60-L63">https://github.com/THU-MAIC/OpenMAIC/blob/v1.0.0/middleware.ts#L60-L63</a><br><a href="https://github.com/THU-MAIC/OpenMAIC/releases/tag/v1.0.1">https://github.com/THU-MAIC/OpenMAIC/releases/tag/v1.0.1</a><br><a href="https://github.com/THU-MAIC/OpenMAIC/security/advisories/GHSA-9m7h-vh2h-rc3w">https://github.com/THU-MAIC/OpenMAIC/security/advisories/GHSA-9m7h-vh2h-rc3w</a><br><a href="https://www.vulncheck.com/advisories/openmaic-before-1.0.1-ssrf-via-environment-gated-url-validation">https://www.vulncheck.com/advisories/openmaic-before-1.0.1-ssrf-via-environment-gated-url-validation</a>                                                                                                                                                                                                                                                                                                                                                                                                                                   |              |             |                  |
| <a href="#">CVE-2026-86428</a> | 7,5       | commonmark                                                        | Inefficient Algorithmic Complexity                                                         | before 2.10.0                      | <a href="https://github.com/thepleague/commonmark/security/advisories/GHSA-8rr7-cvq3-qmfm">https://github.com/thepleague/commonmark/security/advisories/GHSA-8rr7-cvq3-qmfm</a><br><a href="https://www.vulncheck.com/advisories/commonmark-1.5.0-before-2.10.0-denial-of-service-via-attributes">https://www.vulncheck.com/advisories/commonmark-1.5.0-before-2.10.0-denial-of-service-via-attributes</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |              |             |                  |
| <a href="#">CVE-2026-86429</a> | 7,5       | The league/commonmark (thepleague/commonmark) library             | Inefficient Algorithmic Complexity                                                         | >= 1.5; < 2.9                      | <a href="https://github.com/thepleague/commonmark/security/advisories/GHSA-8jv6-8j6v-6j52">https://github.com/thepleague/commonmark/security/advisories/GHSA-8jv6-8j6v-6j52</a><br><a href="https://www.vulncheck.com/advisories/commonmark-before-2.9.1-denial-of-service-via-smartpunct-and-attributes">https://www.vulncheck.com/advisories/commonmark-before-2.9.1-denial-of-service-via-smartpunct-and-attributes</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |              |             |                  |
| <a href="#">CVE-2026-86430</a> | 7,5       | league/commonmark versions                                        | Inefficient Algorithmic Complexity                                                         | versions before 2.9.1              | <a href="https://github.com/thepleague/commonmark/security/advisories/GHSA-8jpm-qj4c-rq4x">https://github.com/thepleague/commonmark/security/advisories/GHSA-8jpm-qj4c-rq4x</a><br><a href="https://www.vulncheck.com/advisories/league-commonmark-before-2.9.1-denial-of-service-via-parsing">https://www.vulncheck.com/advisories/league-commonmark-before-2.9.1-denial-of-service-via-parsing</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |              |             |                  |
| <a href="#">CVE-2026-61409</a> | 7,3       | Dell Secure Connect Gateway (SCG)                                 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | versions prior to 5.36.00.00       | <a href="https://www.dell.com/support/kbdoc/en-in/000503426/dsa-2026-382-security-update-for-dell-secure-connect-gateway-virtual-edition-multiple-vulnerabilities">https://www.dell.com/support/kbdoc/en-in/000503426/dsa-2026-382-security-update-for-dell-secure-connect-gateway-virtual-edition-multiple-vulnerabilities</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |              |             |                  |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                                                                    | Τύπος Ευπάθειας                                                                                                                                                                          | Συσκευές/Εκδόσεις που επηρεάζονται                                                    | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-86261</a> | 7,3       | sfturing hosp_order                                                                                | Improper Authorization; Authorization Bypass Through User-Controlled Key                                                                                                                 | up to 627f426331da8086ce8fff2017d65b1ddef384f8.                                       | <a href="https://github.com/sfturing/hosp_order/">https://github.com/sfturing/hosp_order/</a><br><a href="https://github.com/sfturing/hosp_order/issues/114">https://github.com/sfturing/hosp_order/issues/114</a><br><a href="https://vuldb.com/cve/CVE-2026-86261">https://vuldb.com/cve/CVE-2026-86261</a><br><a href="https://vuldb.com/submit/902240">https://vuldb.com/submit/902240</a><br><a href="https://vuldb.com/vuln/399407">https://vuldb.com/vuln/399407</a><br><a href="https://vuldb.com/vuln/399407/ctj">https://vuldb.com/vuln/399407/ctj</a>                                                                                                                                                                                                                                                                                                                 |              |             |                  |
| <a href="#">CVE-2026-86273</a> | 7,3       | projeto-siga siga                                                                                  | Server-Side Request Forgery (SSRF)                                                                                                                                                       | up to 11.1.1.                                                                         | <a href="https://github.com/projeto-siga/siga/">https://github.com/projeto-siga/siga/</a><br><a href="https://github.com/projeto-siga/siga/issues/2492">https://github.com/projeto-siga/siga/issues/2492</a><br><a href="https://vuldb.com/cve/CVE-2026-86273">https://vuldb.com/cve/CVE-2026-86273</a><br><a href="https://vuldb.com/submit/904863">https://vuldb.com/submit/904863</a><br><a href="https://vuldb.com/vuln/399434">https://vuldb.com/vuln/399434</a><br><a href="https://vuldb.com/vuln/399434/ctj">https://vuldb.com/vuln/399434/ctj</a>                                                                                                                                                                                                                                                                                                                       |              |             |                  |
| <a href="#">CVE-2026-86276</a> | 7,3       | SourceCodester Syllabus-Aligned Learning Management & Examination System                           | Use of Hard-coded Password; Use of Hard-coded Credentials                                                                                                                                | 1.0                                                                                   | <a href="https://github.com/hackliu/Vulnerability-Reports/blob/master/Syllabus%20Aligned%20Learning%20Management%20Examination%20System/VULN-03-SQL-Injection-Hardcoded-Credentials.md">https://github.com/hackliu/Vulnerability-Reports/blob/master/Syllabus%20Aligned%20Learning%20Management%20Examination%20System/VULN-03-SQL-Injection-Hardcoded-Credentials.md</a><br><a href="https://vuldb.com/cve/CVE-2026-86276">https://vuldb.com/cve/CVE-2026-86276</a><br><a href="https://vuldb.com/submit/904873">https://vuldb.com/submit/904873</a><br><a href="https://vuldb.com/vuln/399437">https://vuldb.com/vuln/399437</a><br><a href="https://vuldb.com/vuln/399437/ctj">https://vuldb.com/vuln/399437/ctj</a><br><a href="https://www.sourcecodester.com/">https://www.sourcecodester.com/</a>                                                                         |              |             |                  |
| <a href="#">CVE-2026-86282</a> | 7,3       | jaychouchannel Tourism-Management-System                                                           | Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | up to 8122bf020d91199eddf3ee02d1632a70a9a132.                                         | <a href="https://github.com/jaychouchannel/Tourism-Management-System/">https://github.com/jaychouchannel/Tourism-Management-System/</a><br><a href="https://github.com/jaychouchannel/Tourism-Management-System/commit/d44ec3aa0bd2a72c8800e3befb0a9a96a6491986">https://github.com/jaychouchannel/Tourism-Management-System/commit/d44ec3aa0bd2a72c8800e3befb0a9a96a6491986</a><br><a href="https://github.com/jaychouchannel/Tourism-Management-System/pull/14">https://github.com/jaychouchannel/Tourism-Management-System/pull/14</a><br><a href="https://github.com/jaychouchannel/Tourism-Management-System/issues/7">https://github.com/jaychouchannel/Tourism-Management-System/issues/7</a><br><a href="https://vuldb.com/cve/CVE-2026-86282">https://vuldb.com/cve/CVE-2026-86282</a><br><a href="https://vuldb.com/submit/905639">https://vuldb.com/submit/905639</a> |              |             |                  |
| <a href="#">CVE-2026-86292</a> | 7,3       | SourceCodester Simple Traffic Offense System                                                       | Improper Authentication; Missing Authentication for Critical Function                                                                                                                    | 1.0                                                                                   | <a href="https://github.com/tan1540684326-OAO/cve/issues/1">https://github.com/tan1540684326-OAO/cve/issues/1</a><br><a href="https://vuldb.com/cve/CVE-2026-86292">https://vuldb.com/cve/CVE-2026-86292</a><br><a href="https://vuldb.com/submit/906272">https://vuldb.com/submit/906272</a><br><a href="https://vuldb.com/vuln/399454">https://vuldb.com/vuln/399454</a><br><a href="https://vuldb.com/vuln/399454/ctj">https://vuldb.com/vuln/399454/ctj</a><br><a href="https://www.sourcecodester.com/">https://www.sourcecodester.com/</a>                                                                                                                                                                                                                                                                                                                                 |              |             |                  |
| <a href="#">CVE-2026-86300</a> | 7,3       | Tenda AC9                                                                                          | Improper Authentication                                                                                                                                                                  | 15.03.05.14                                                                           | <a href="https://github.com/limou89/somevul/blob/main/Tenda_AC9_fast_setting_wifi_set_Unauth_Password.md">https://github.com/limou89/somevul/blob/main/Tenda_AC9_fast_setting_wifi_set_Unauth_Password.md</a><br><a href="https://github.com/limou89/somevul/blob/main/Tenda_AC9_qetProduct_Info_Disclosure.md">https://github.com/limou89/somevul/blob/main/Tenda_AC9_qetProduct_Info_Disclosure.md</a><br><a href="https://vuldb.com/cve/CVE-2026-86300">https://vuldb.com/cve/CVE-2026-86300</a><br><a href="https://vuldb.com/submit/906606">https://vuldb.com/submit/906606</a><br><a href="https://vuldb.com/submit/906607">https://vuldb.com/submit/906607</a><br><a href="https://vuldb.com/submit/906608">https://vuldb.com/submit/906608</a>                                                                                                                           |              |             |                  |
| <a href="#">CVE-2026-86303</a> | 7,3       | 92181 markdown                                                                                     | Improper Restriction of Operations within the Bounds of a Memory Buffer; Out-of-bounds Read                                                                                              | up to 058cab0cb7fb245a0ccc6b8446963ff8d573558f.                                       | <a href="https://github.com/92181/markdown/">https://github.com/92181/markdown/</a><br><a href="https://github.com/92181/markdown/commit/c000d2f9cf390c315378d3717cf20911cf3e80a6">https://github.com/92181/markdown/commit/c000d2f9cf390c315378d3717cf20911cf3e80a6</a><br><a href="https://github.com/92181/markdown/issues/1">https://github.com/92181/markdown/issues/1</a><br><a href="https://github.com/92181/markdown/pull/2">https://github.com/92181/markdown/pull/2</a><br><a href="https://vuldb.com/cve/CVE-2026-86303">https://vuldb.com/cve/CVE-2026-86303</a><br><a href="https://vuldb.com/submit/907499">https://vuldb.com/submit/907499</a>                                                                                                                                                                                                                   |              |             |                  |
| <a href="#">CVE-2026-86305</a> | 7,3       | light0011 cms<br>c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930 | Improper Access Control; Unrestricted Upload of File with Dangerous Type                                                                                                                 | c774dce31c6df0055568a8d5c53d964d99be199d;<br>f72cf46f601efb2a0618c3814cc2f61380b38930 | <a href="https://github.com/light0011/cms/">https://github.com/light0011/cms/</a><br><a href="https://github.com/light0011/cms/issues/9">https://github.com/light0011/cms/issues/9</a><br><a href="https://vuldb.com/cve/CVE-2026-86305">https://vuldb.com/cve/CVE-2026-86305</a><br><a href="https://vuldb.com/submit/894804">https://vuldb.com/submit/894804</a><br><a href="https://vuldb.com/vuln/399478">https://vuldb.com/vuln/399478</a><br><a href="https://vuldb.com/vuln/399478/ctj">https://vuldb.com/vuln/399478/ctj</a>                                                                                                                                                                                                                                                                                                                                             |              |             |                  |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                                                                                     | Τύπος Ευπάθειας                                                                      | Συσκευές/Εκδόσεις που επηρεάζονται | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-15984</a> | 7,2       | The QuickCal plugin for WordPress                                                                                   | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 1.0.20       | <a href="https://codecanyon.net/item/quickcal-appointment-booking-calendar-for-wordpress/47981746">https://codecanyon.net/item/quickcal-appointment-booking-calendar-for-wordpress/47981746</a><br><a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/9bfcfc13-ccfb-4319-99a7-7d7510a11cfe?source=cve">https://www.wordfence.com/threat-intel/vulnerabilities/id/9bfcfc13-ccfb-4319-99a7-7d7510a11cfe?source=cve</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |              |             |                  |
| <a href="#">CVE-2026-16649</a> | 7,2       | The Gravity Forms plugin for WordPress                                                                              | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 2.10.5       | <a href="https://docs.gravityforms.com/gravityforms-change-log/">https://docs.gravityforms.com/gravityforms-change-log/</a><br><a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/187a420d-a5a5-4b0e-945b-c5694243e68f?source=cve">https://www.wordfence.com/threat-intel/vulnerabilities/id/187a420d-a5a5-4b0e-945b-c5694243e68f?source=cve</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |              |             |                  |
| <a href="#">CVE-2026-18406</a> | 7,2       | The SureForms – Contact Form Builder, AI Forms, Payment Form, Survey & Quiz plugin for WordPress                    | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 2.12.2       | <a href="https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/assets/build/entries.js#L172">https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/assets/build/entries.js#L172</a><br><a href="https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/inc/form-submit.php#L1451">https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/inc/form-submit.php#L1451</a><br><a href="https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/inc/form-submit.php#L229">https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/inc/form-submit.php#L229</a><br><a href="https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/inc/form-submit.php#L93">https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/inc/form-submit.php#L93</a><br><a href="https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/inc/helper.php#L241">https://plugins.trac.wordpress.org/browser/sureforms/tags/2.12.2/inc/helper.php#L241</a><br><a href="https://plugins.trac.wordpress.org/changeset/3635980/sureforms/trunk/inc/form-submit.php">https://plugins.trac.wordpress.org/changeset/3635980/sureforms/trunk/inc/form-submit.php</a>                                                                                                                                                                                                                                                                                                           | none         | no          | partial          |
| <a href="#">CVE-2026-19769</a> | 7,2       | The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress                                 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 3.15.1       | <a href="https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.14.11/includes/AJAX/Controllers/Submission.php#L303">https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.14.11/includes/AJAX/Controllers/Submission.php#L303</a><br><a href="https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.14.11/includes/AJAX/Controllers/Submission.php#L55">https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.14.11/includes/AJAX/Controllers/Submission.php#L55</a><br><a href="https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.14.11/includes/AJAX/Controllers/Submission.php#L609">https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.14.11/includes/AJAX/Controllers/Submission.php#L609</a><br><a href="https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.14.11/includes/AJAX/Controllers/Submission.php#L61">https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.14.11/includes/AJAX/Controllers/Submission.php#L61</a><br><a href="https://plugins.trac.wordpress.org/changeset/3674413/ninja-forms/trunk/includes/AJAX/Controllers/Submission.php">https://plugins.trac.wordpress.org/changeset/3674413/ninja-forms/trunk/includes/AJAX/Controllers/Submission.php</a><br><a href="https://plugins.trac.wordpress.org/changeset?old_path=%2Fninja-forms/tags/3.15.1&amp;new_path=%2Fninja-forms/tags/3.15.2">https://plugins.trac.wordpress.org/changeset?old_path=%2Fninja-forms/tags/3.15.1&amp;new_path=%2Fninja-forms/tags/3.15.2</a> |              |             |                  |
| <a href="#">CVE-2026-6431</a>  | 7,2       | The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 3.15.7       | <a href="https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.15.6/features/email-confirmation/class-email-confirmation.php#L95">https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.15.6/features/email-confirmation/class-email-confirmation.php#L95</a><br><a href="https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.15.6/front-end/class-formbuilder.php#L743">https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.15.6/front-end/class-formbuilder.php#L743</a><br><a href="https://plugins.trac.wordpress.org/browser/profile-builder/trunk/features/email-confirmation/class-email-confirmation.php#L95">https://plugins.trac.wordpress.org/browser/profile-builder/trunk/features/email-confirmation/class-email-confirmation.php#L95</a><br><a href="https://plugins.trac.wordpress.org/browser/profile-builder/trunk/front-end/class-formbuilder.php#L743">https://plugins.trac.wordpress.org/browser/profile-builder/trunk/front-end/class-formbuilder.php#L743</a><br><a href="https://plugins.trac.wordpress.org/changeset/3511465">https://plugins.trac.wordpress.org/changeset/3511465</a><br><a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/99e6cc7b-7e65-4b8d-a927-1329ed6c1954?source=cve">https://www.wordfence.com/threat-intel/vulnerabilities/id/99e6cc7b-7e65-4b8d-a927-1329ed6c1954?source=cve</a>                                                                                                                         |              |             |                  |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                                                                                | Τύπος Ευπάθειας                                                                      | Συσκευές/Εκδόσεις που επηρεάζονται | URL οδηγιών αντιμετώπισης                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-77233</a> | 7,2       | The iubenda   All-in-one Compliance for GDPR / CCPA Cookie Consent + more plugin for WordPress | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 3.13.4       | <a href="https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.2/iubenda-cookie-class/iubenda.class.php#L557">https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.2/iubenda-cookie-class/iubenda.class.php#L557</a><br><a href="https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.2/iubenda-cookie-class/iubenda.class.php#L570">https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.2/iubenda-cookie-class/iubenda.class.php#L570</a><br><a href="https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.2/iubenda_cookie_solution.php#L986">https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.2/iubenda_cookie_solution.php#L986</a><br><a href="https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.3/iubenda-cookie-class/iubenda.class.php#L557">https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.3/iubenda-cookie-class/iubenda.class.php#L557</a><br><a href="https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.3/iubenda-cookie-class/iubenda.class.php#L570">https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.3/iubenda-cookie-class/iubenda.class.php#L570</a><br><a href="https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.3/iubenda_cookie_solution.php#L986">https://plugins.trac.wordpress.org/browser/iubenda-cookie-law-solution/tags/3.13.3/iubenda_cookie_solution.php#L986</a> |              |             |                  |
| <a href="#">CVE-2026-77830</a> | 7,2       | The Spam protection, Honeypot, Anti-Spam by CleanTalk plugin for WordPress                     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 6.86         | <a href="https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.84/cleantalk.php#L234">https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.84/cleantalk.php#L234</a><br><a href="https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.84/lib/Cleantalk/ApiWP/ContactsEncoder/ContactsEncoder.php#L114">https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.84/lib/Cleantalk/ApiWP/ContactsEncoder/ContactsEncoder.php#L114</a><br><a href="https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.84/lib/Cleantalk/Common/ContactsEncoder/ContactsEncoder.php#L914">https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.84/lib/Cleantalk/Common/ContactsEncoder/ContactsEncoder.php#L914</a><br><a href="https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.84/lib/Cleantalk/Common/ContactsEncoder/ContactsEncoder.php#L933">https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.84/lib/Cleantalk/Common/ContactsEncoder/ContactsEncoder.php#L933</a><br><a href="https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.85/cleantalk.php#L234">https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.85/cleantalk.php#L234</a><br><a href="https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.85/lib/Cleantalk/ApiWP/ContactsEncoder/ContactsEncoder.php#L114">https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.85/lib/Cleantalk/ApiWP/ContactsEncoder/ContactsEncoder.php#L114</a> |              |             |                  |
| <a href="#">CVE-2026-78438</a> | 7,2       | The W3 Total Cache plugin for WordPress                                                        | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 2.10.5       | <a href="https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.5/UserExperience/LazyLoad/Mutator.php#L255">https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.5/UserExperience/LazyLoad/Mutator.php#L255</a><br><a href="https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.5/UserExperience/LazyLoad/Mutator.php#L293">https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.5/UserExperience/LazyLoad/Mutator.php#L293</a><br><a href="https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.5/UserExperience/LazyLoad/Mutator.php#L91">https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.5/UserExperience/LazyLoad/Mutator.php#L91</a><br><a href="https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.6/UserExperience/LazyLoad/Plugin.php#L87">https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.6/UserExperience/LazyLoad/Plugin.php#L87</a><br><a href="https://plugins.trac.wordpress.org/changeset/3680101/w3-total-cache/tags/2.10.6/UserExperience/LazyLoad/Mutator.php">https://plugins.trac.wordpress.org/changeset/3680101/w3-total-cache/tags/2.10.6/UserExperience/LazyLoad/Mutator.php</a><br><a href="https://plugins.trac.wordpress.org/changeset?old_path=%2Fw3-total-cache/tags/2.10.5&amp;new_path=%2Fw3-total-cache/tags/2.10.6">https://plugins.trac.wordpress.org/changeset?old_path=%2Fw3-total-cache/tags/2.10.5&amp;new_path=%2Fw3-total-cache/tags/2.10.6</a>                                                                                                                 | none         | no          | partial          |
| <a href="#">CVE-2026-83625</a> | 7,2       | The Contact Form by Supsysic plugin for WordPress                                              | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 1.10.2       | <a href="https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/classes/utlis.php#L77">https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/classes/utlis.php#L77</a><br><a href="https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/modules/forms/controller.php#L390">https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/modules/forms/controller.php#L390</a><br><a href="https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/modules/forms/controller.php#L411">https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/modules/forms/controller.php#L411</a><br><a href="https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/modules/forms/is/admin.forms.contacts.list.is#L204">https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/modules/forms/is/admin.forms.contacts.list.is#L204</a><br><a href="https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/modules/forms/models/forms.php#L103">https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.10.2/modules/forms/models/forms.php#L103</a><br><a href="https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.8.1/classes/utlis.php#L77">https://plugins.trac.wordpress.org/browser/contact-form-by-supsysic/tags/1.8.1/classes/utlis.php#L77</a>                                                                                                                             | none         | yes         | partial          |

| URL ευπάθειας (NIST NVD)       | CVSS v3.1 | Προϊόν/Υπηρεσία                            | Τύπος Ευπάθειας                                                                      | Συσκευές/Εκδόσεις που επηρεάζονται | URL οδηγιών αντιμετώπισης                                                                                                                                   | Exploitation | Automatable | Technical Impact |
|--------------------------------|-----------|--------------------------------------------|--------------------------------------------------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|------------------|
| <a href="#">CVE-2026-81404</a> | 7,1       | The IPGP Visitors Origin Word-Press plugin | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | before 1.6                         | <a href="https://wpscan.com/vulnerability/8fbfb296-78d8-4f3b-ab21-7a5a4e0ea421/">https://wpscan.com/vulnerability/8fbfb296-78d8-4f3b-ab21-7a5a4e0ea421/</a> | none         | no          | partial          |

## CISA/CERT-EU Alerts & Advisories

- 🔍 Αυτό το κομμάτι περιλαμβάνει ειδοποιήσεις από επίσημες πηγές, κυρίως CISA και CERT-EU, σχετικά με κρίσιμες ευπάθειες ή ενεργές απειλές. Συνήθως αφορούν βιομηχανικά ή κρίσιμα συστήματα, αλλά και mainstream λογισμικό. Προσφέρονται σε μορφή σύντομων αναφορών και οδηγούν σε πιο λεπτομερείς τεχνικές οδηγίες.

| Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες |   | URL |
|-------------------------------------------------|---|-----|
| -                                               | - | -   |

## News

Η ενότητα "News" συνοψίζει τα πιο σημαντικά γεγονότα της εβδομάδας στον τομέα της κυβερνοασφάλειας. Εδώ θα βρείτε επιθέσεις που ξεχώρισαν, νέες τεχνικές που εντοπίστηκαν, ή ενέργειες από γνωστές ομάδες hacking. Δίνει την απαραίτητη εικόνα του τι συμβαίνει διεθνώς και πού πρέπει να στραφεί η προσοχή.

| Σύντομη περιγραφή / Τίτλος                                                                        | URL                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New InjectEave Attack Allows Hackers to Recover Audio Playing on Headphones from 30 Meters        | <a href="https://cybersecuritynews.com/injecteave-attack">https://cybersecuritynews.com/injecteave-attack</a>                                                                                             |
| Switzerland Moves Away From Microsoft 365 to Open-Source Alternatives                             | <a href="https://cybersecuritynews.com/switzerland-moves-away-from-microsoft-365">https://cybersecuritynews.com/switzerland-moves-away-from-microsoft-365</a>                                             |
| Natural Resources Wales Exposes Sensitive Employee Data in Spreadsheet Breach                     | <a href="https://cybersecuritynews.com/natural-resources-wales-expose">https://cybersecuritynews.com/natural-resources-wales-expose</a>                                                                   |
| Microsoft to Retire Manifest V2 Extensions and Switch to V3 for Improved Security and Performance | <a href="https://cybersecuritynews.com/microsoft-to-retire-manifest-v2-extensions">https://cybersecuritynews.com/microsoft-to-retire-manifest-v2-extensions</a>                                           |
| New Linux Bot Hides as Kernel Process and Launches DDoS Attacks                                   | <a href="https://cybersecuritynews.com/new-linux-bot">https://cybersecuritynews.com/new-linux-bot</a>                                                                                                     |
| NCSC Warns Shadow AI Creates New Security Risks                                                   | <a href="https://infosecurity-magazine.com/news/ncsc-warns-shadow-ai-security-risks">https://infosecurity-magazine.com/news/ncsc-warns-shadow-ai-security-risks</a>                                       |
| LG Smart TVs Caught Scanning Networks and Logging Audio in Standby                                | <a href="https://cybersecuritynews.com/lq-smart-tvs-caught-scanning-networks">https://cybersecuritynews.com/lq-smart-tvs-caught-scanning-networks</a>                                                     |
| Why Are So Many Security Professionals Keeping Breaches Quiet?                                    | <a href="https://thehackernews.com/expert-insights/2026/09/why-are-so-many-security-professionals.html">https://thehackernews.com/expert-insights/2026/09/why-are-so-many-security-professionals.html</a> |
| OpenAI Agents Hijack Another Victim Website                                                       | <a href="https://securityweek.com/openai-agents-hijack-another-victim-website">https://securityweek.com/openai-agents-hijack-another-victim-website</a>                                                   |

| Σύντομη περιγραφή / Τίτλος                                                                      | URL                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rhysida Publishes Berlin Government Data After €2m Extortion Demand Re</b>                   | <a href="https://infosecurity-magazine.com/news/rhysida-berlin-data-extortion">https://infosecurity-magazine.com/news/rhysida-berlin-data-extortion</a>                                                                                                                     |
| <b>Rogue ScreenConnect Clients Spread Four-Stage VBScript Chain to Newly Connected Hosts</b>    | <a href="https://thehackernews.com/2026/09/rogue-screenconnect-clients-spread-four.html">https://thehackernews.com/2026/09/rogue-screenconnect-clients-spread-four.html</a>                                                                                                 |
| <b>North Korea's Lazarus Operates Through Six Distinct Cyber Clusters</b>                       | <a href="https://infosecurity-magazine.com/news/north-korea-lazarus-six-cyber">https://infosecurity-magazine.com/news/north-korea-lazarus-six-cyber</a>                                                                                                                     |
| <b>ChatGPT can now connect to your personal apps to mimic writing style</b>                     | <a href="https://bleepingcomputer.com/news/artificial-intelligence/chatgpt-can-now-connect-to-your-personal-apps-to-mimic-writing-style">https://bleepingcomputer.com/news/artificial-intelligence/chatgpt-can-now-connect-to-your-personal-apps-to-mimic-writing-style</a> |
| <b>Multiple Class Action Lawsuits Filed Against IDScan</b>                                      | <a href="https://infosecurity-magazine.com/news/multiple-class-action-lawsuits">https://infosecurity-magazine.com/news/multiple-class-action-lawsuits</a>                                                                                                                   |
| <b>Malicious Chrome Extension Can Steal Login Sessions and Turn PCs Into Remote Backdoors</b>   | <a href="https://cybersecuritynews.com/malicious-chrome-extension-2">https://cybersecuritynews.com/malicious-chrome-extension-2</a>                                                                                                                                         |
| <b>Privacy Policy</b>                                                                           | <a href="https://cybersecuritynews.com/privacy-policy-2">https://cybersecuritynews.com/privacy-policy-2</a>                                                                                                                                                                 |
| <b>Blind Spots and Backdoors: Practical Advice for Identity Risk Reduction</b>                  | <a href="https://thehackernews.com/expert-insights/2026/09/blind-spots-and-backdoors-practical.html">https://thehackernews.com/expert-insights/2026/09/blind-spots-and-backdoors-practical.html</a>                                                                         |
| <b>The Economics of Dwell Time and Why AI Native SIEM Changes the Equation</b>                  | <a href="https://thehackernews.com/expert-insights/2026/09/the-economics-of-dwell-time-and-why-ai.html">https://thehackernews.com/expert-insights/2026/09/the-economics-of-dwell-time-and-why-ai.html</a>                                                                   |
| <b>ChatGPT Astra is now rolling out to \$20 Plus subscription</b>                               | <a href="https://bleepingcomputer.com/news/artificial-intelligence/chatgpt-astra-is-now-rolling-out-to-20-plus-subscription">https://bleepingcomputer.com/news/artificial-intelligence/chatgpt-astra-is-now-rolling-out-to-20-plus-subscription</a>                         |
| <b>CrowdStrike Launches SafeMind - First Agentic Cybersecurity Solution Built for Defenders</b> | <a href="https://cybersecuritynews.com/crowdstrike-launches-safemind">https://cybersecuritynews.com/crowdstrike-launches-safemind</a>                                                                                                                                       |

## Breaches / Compromised / Hacked

Καταγράφονται περιπτώσεις παραβίασης δεδομένων, διαρροών και άλλων σοβαρών περιστατικών ασφαλείας. Περιλαμβάνονται πληροφορίες για το ποιοι επηρεάστηκαν, με ποιον τρόπο έγινε η παραβίαση και πού υπάρχουν διαθέσιμες λεπτομέρειες. Είναι μια χρήσιμη εικόνα για να αντιληφθεί κανείς τη δυναμική των επιθέσεων σε πραγματικές συνθήκες.

| Σύντομη περιγραφή / Τίτλος                                                                    | URL                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bimbo Bakeries USA Confirms Data Breach in Oracle EBS Zero-Day Attack</b>                  | <a href="https://cybersecuritynews.com/bimbo-oracle-ebs-data-breach">https://cybersecuritynews.com/bimbo-oracle-ebs-data-breach</a>                                                                                                                   |
| <b>Online Maths Learning Platform Mathspace Disclosed Data Breach Impacts 1 Million Users</b> | <a href="https://cybersecuritynews.com/mathspace-data-breach">https://cybersecuritynews.com/mathspace-data-breach</a>                                                                                                                                 |
| <b>Mathspace discloses data breach affecting over 1 million people</b>                        | <a href="https://bleepingcomputer.com/news/security/mathspace-discloses-data-breach-affecting-over-1-million-people">https://bleepingcomputer.com/news/security/mathspace-discloses-data-breach-affecting-over-1-million-people</a>                   |
| <b>Trezor data breach impact now reaches 81,000 customers</b>                                 | <a href="https://bleepingcomputer.com/news/security/trezor-data-breach-impact-now-reaches-81-000-customers">https://bleepingcomputer.com/news/security/trezor-data-breach-impact-now-reaches-81-000-customers</a>                                     |
| <b>Over 5,400 hacked sites serve ClickFix payloads stored on the blockchain</b>               | <a href="https://bleepingcomputer.com/news/security/over-5-400-hacked-sites-serve-clickfix-payloads-stored-on-the-blockchain">https://bleepingcomputer.com/news/security/over-5-400-hacked-sites-serve-clickfix-payloads-stored-on-the-blockchain</a> |

## Vulnerabilities / Flaws / Zero-day

Αναφέρονται τεχνικά ελαττώματα ή αδυναμίες που ενδέχεται να αξιοποιηθούν άμεσα από επιτιθέμενους — είτε επειδή είναι zero-day είτε γιατί η διόρθωσή τους καθυστερεί. Περιλαμβάνονται περιπτώσεις όπου δεν απαιτείται αλληλεπίδραση με τον χρήστη ή όπου παρακάμπτονται βασικά μέτρα ασφαλείας. Πολύ χρήσιμο για ομάδες που ασχολούνται με threat detection.

| Σύντομη περιγραφή / Τίτλος                                                                            | URL                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ConnectWise Warns of New ScreenConnect Remote Access Flaw - Released Mitigation Steps</b>          | <a href="https://cybersecuritynews.com/connectwise-screenconnect-remote-access-flaw">https://cybersecuritynews.com/connectwise-screenconnect-remote-access-flaw</a>                                                             |
| <b>Nightmare Eclipse Drops CrowdStrike, Nvidia, Avast Zero-Day Exploits</b>                           | <a href="https://securityweek.com/nightmare-eclipse-drops-crowdstrike-nvidia-avast-zero-day-exploits">https://securityweek.com/nightmare-eclipse-drops-crowdstrike-nvidia-avast-zero-day-exploits</a>                           |
| <b>Telerik UI Padding-Oracle Bug Chained to Unauthenticated RCE — Public Exploit Released</b>         | <a href="https://thehackernews.com/2026/09/telerik-ui-padding-oracle-bug-chained.html">https://thehackernews.com/2026/09/telerik-ui-padding-oracle-bug-chained.html</a>                                                         |
| <b>Hackers exploit new MikroTik RouterOS flaws to hijack routers</b>                                  | <a href="https://bleepingcomputer.com/news/security/hackers-exploit-new-mikrotik-routeros-flaws-to-hijack-routers">https://bleepingcomputer.com/news/security/hackers-exploit-new-mikrotik-routeros-flaws-to-hijack-routers</a> |
| <b>ConnectWise warns of new ScreenConnect flaw without patch</b>                                      | <a href="https://bleepingcomputer.com/news/security/connectwise-warns-of-new-screenconnect-flaw-without-patch">https://bleepingcomputer.com/news/security/connectwise-warns-of-new-screenconnect-flaw-without-patch</a>         |
| <b>N-able Issues Fourth N-central Hotfix in Five Weeks for Unauthenticated RCE Flaw</b>               | <a href="https://thehackernews.com/2026/09/n-able-issues-fourth-n-central-hotfix.html">https://thehackernews.com/2026/09/n-able-issues-fourth-n-central-hotfix.html</a>                                                         |
| <b>Researcher Shares CrowdStrike Privilege Escalation Zero Day</b>                                    | <a href="https://infosecurity-magazine.com/news/crowdstrike-privilege-escalation">https://infosecurity-magazine.com/news/crowdstrike-privilege-escalation</a>                                                                   |
| <b>Critical Software Vulnerabilities Surge From Under 100 to More Than 600 a Month</b>                | <a href="https://cybersecuritynews.com/critical-software-vulnerabilities-surge">https://cybersecuritynews.com/critical-software-vulnerabilities-surge</a>                                                                       |
| <b>12-Year-Old PostgreSQL Flaw Lets Attackers Execute Code on Database Servers</b>                    | <a href="https://cybersecuritynews.com/12-year-old-postgresql-flaw">https://cybersecuritynews.com/12-year-old-postgresql-flaw</a>                                                                                               |
| <b>ASUS Control Center Flaw Allows Attackers to Gain Full Admin Control of the System</b>             | <a href="https://cybersecuritynews.com/asus-control-center-vulnerability">https://cybersecuritynews.com/asus-control-center-vulnerability</a>                                                                                   |
| <b>Hackers Exploiting MikroTik RouterOS Vulnerability in the Wild to Gain Complete Network Access</b> | <a href="https://cybersecuritynews.com/mikrotik-routeros-vulnerability">https://cybersecuritynews.com/mikrotik-routeros-vulnerability</a>                                                                                       |
| <b>Hackers Actively Exploiting Magento and Adobe Commerce 0-Day RCE Vulnerability</b>                 | <a href="https://cybersecuritynews.com/magento-and-adobe-commerce-0-day-rce">https://cybersecuritynews.com/magento-and-adobe-commerce-0-day-rce</a>                                                                             |
| <b>Critical VMware Workstation and Fusion Flaw Lets VM Admins Execute Host Code</b>                   | <a href="https://thehackernews.com/2026/09/critical-vmware-workstation-and-fusion.html">https://thehackernews.com/2026/09/critical-vmware-workstation-and-fusion.html</a>                                                       |
| <b>Elementor Pro WordPress Plugin Vulnerability Exploited to Hack Sites</b>                           | <a href="https://securityweek.com/elementor-pro-wordpress-plugin-vulnerability-exploited-to-hack-sites">https://securityweek.com/elementor-pro-wordpress-plugin-vulnerability-exploited-to-hack-sites</a>                       |
| <b>Attackers Exploit PaperCut Flaws to Steal Credentials From Schools and Universities</b>            | <a href="https://thehackernews.com/2026/09/attackers-exploit-papercut-flaws-to.html">https://thehackernews.com/2026/09/attackers-exploit-papercut-flaws-to.html</a>                                                             |

## Patches / Updates / Fixes

Εδώ θα βρείτε τις πιο πρόσφατες διορθώσεις και ενημερώσεις ασφαλείας από προμηθευτές λογισμικού και hardware. Το περιεχόμενο αφορά συγκεκριμένα bugs ή exploits που έχουν ήδη δημοσιοποιηθεί, μαζί με οδηγίες για το πώς να εφαρμοστούν τα patches.

| Σύντομη περιγραφή / Τίτλος                                                               | URL                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>N-able Releases Hotfix for Critical Remote Code Execution Flaw</b>                    | <a href="https://infosecurity-magazine.com/news/nable-hotfix-critical-rce">https://infosecurity-magazine.com/news/nable-hotfix-critical-rce</a>                                                                                     |
| <b>OpenVPN Fixes 7 Security Flaws Affecting VPN Connections and Windows Systems</b>      | <a href="https://cybersecuritynews.com/openvpn-fixes-7-security-flaws">https://cybersecuritynews.com/openvpn-fixes-7-security-flaws</a>                                                                                             |
| <b>N-able patches max severity N-central flaw amid ongoing attacks</b>                   | <a href="https://bleepingcomputer.com/news/security/n-able-patches-max-severity-n-central-flaw-amid-ongoing-attacks">https://bleepingcomputer.com/news/security/n-able-patches-max-severity-n-central-flaw-amid-ongoing-attacks</a> |
| <b>Unpatched Magento and Adobe Commerce Zero-Day Exploited to Backdoor Online Stores</b> | <a href="https://thehackernews.com/2026/09/unpatched-magento-and-adobe-commerce.html">https://thehackernews.com/2026/09/unpatched-magento-and-adobe-commerce.html</a>                                                               |

## Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συν-θήκες. Περιλαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

| Σύντομη περιγραφή / Τίτλος                                                                | URL                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Shai-Hulud npm Worm Resurfaces After 111 Days and Slips Past Malware Scanning</b>      | <a href="https://cybersecuritynews.com/shai-hulud-npm-worm">https://cybersecuritynews.com/shai-hulud-npm-worm</a>                                                                                                                                     |
| <b>Magento StyleSmuggler zero-day exploited to deploy Linux backdoor</b>                  | <a href="https://bleepingcomputer.com/news/security/magento-stylesmuggler-zero-day-exploited-to-deploy-linux-backdoor">https://bleepingcomputer.com/news/security/magento-stylesmuggler-zero-day-exploited-to-deploy-linux-backdoor</a>               |
| <b>BigBear Microsoft 365 phishing service bypassed MFA at 258 organizations</b>           | <a href="https://bleepingcomputer.com/news/security/bigbear-microsoft-365-phishing-service-bypassed-mfa-at-258-organizations">https://bleepingcomputer.com/news/security/bigbear-microsoft-365-phishing-service-bypassed-mfa-at-258-organizations</a> |
| <b>Linux Rootkit Injects Fileless PHP Web Shells Into Compromised F5 BIG-IP Servers</b>   | <a href="https://cybersecuritynews.com/linux-rootkit">https://cybersecuritynews.com/linux-rootkit</a>                                                                                                                                                 |
| <b>Hackers Abuse Trusted Google Services to Hide Credential-Stealing Phishing Attacks</b> | <a href="https://cybersecuritynews.com/trusted-google-services">https://cybersecuritynews.com/trusted-google-services</a>                                                                                                                             |
| <b>⚡ Weekly Recap: Chrome 0-Day, Router Hijacks, Coder Supply Chain Attack and More</b>   | <a href="https://thehackernews.com/2026/09/weekly-recap-chrome-0-day-router.html">https://thehackernews.com/2026/09/weekly-recap-chrome-0-day-router.html</a>                                                                                         |
| <b>Adobe Commerce Zero-Day Exploited to Backdoor Online Stores</b>                        | <a href="https://securityweek.com/adobe-commerce-zero-day-exploited-to-backdoor-online-stores">https://securityweek.com/adobe-commerce-zero-day-exploited-to-backdoor-online-stores</a>                                                               |
| <b>Modified ScreenConnect Clients Used in Worm-Like Campaign</b>                          | <a href="https://securityweek.com/modified-screenconnect-clients-used-in-worm-like-campaign">https://securityweek.com/modified-screenconnect-clients-used-in-worm-like-campaign</a>                                                                   |
| <b>Russian Hackers Use New HOOKEDGE Backdoor to Spy on European Organizations</b>         | <a href="https://cybersecuritynews.com/russian-hackers-use-new-hookedge">https://cybersecuritynews.com/russian-hackers-use-new-hookedge</a>                                                                                                           |
| <b>Attackers conceal phishing lures using invisible Unicode characters</b>                | <a href="https://bleepingcomputer.com/news/security/attackers-conceal-phishing-lures-using-invisible-unicode-characters">https://bleepingcomputer.com/news/security/attackers-conceal-phishing-lures-using-invisible-unicode-characters</a>           |

## Guides / Tools

Παρουσιάζονται τεχνικοί οδηγοί και εργαλεία που μπορούν να βοηθήσουν στην παρακολούθηση, ανάλυση ή ενίσχυση της ασφάλειας συστημάτων. Είτε πρόκειται για open source projects είτε για νέες τεχνικές, η ενότητα αυτή λειτουργεί ως πόρος για πρακτικές λύσεις στην καθημερινή δουλειά των επαγγελματιών ασφάλειας.

| Σύντομη περιγραφή / Τίτλος                              | URL                                                                                                                                                                             |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| North Korean Hackers Deploy New Linux Espionage Toolkit | <a href="https://securityweek.com/north-korean-hackers-deploy-new-linux-espionage-toolkit">https://securityweek.com/north-korean-hackers-deploy-new-linux-espionage-toolkit</a> |

## References

- [1]. Ο βαθμός επικινδυνότητας είναι σύμφωνα με την κλίμακα Common Vulnerability Scoring System (CVSSv3), <https://nvd.nist.gov/vuln-metrics/cvss>
- [2]. Τα CVEs αποτελέσματα που εμφανίζονται στην ενότητα 1 διαθέτουν CVSS v3.1 score  $\geq 7.0$ , αφορούν το διάστημα 05/09/2026–08/09/2026, και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

## Annex – Websites with vendor specific vulnerabilities

Ο πίνακας περιέχει websites από κατασκευαστές που προσφέρουν πληροφορίες σχετικές με ευπάθειες που εμφανίζονται στα προϊόντα τους.

| Vendor name / Platform | URL                                                                                                                                                                                                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wordpress              | Wordfence Intelligence Vulnerability Database API <a href="https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/">https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/</a><br>Scan your WordPress website, <a href="https://wpscan.com/scan/">https://wpscan.com/scan/</a> |
| Oracle                 | Critical Patch Updates, Security Alerts and Bulletins, <a href="https://www.oracle.com/security-alerts/">https://www.oracle.com/security-alerts/</a>                                                                                                                                                                |
| Fortinet               | Fortinet products, <a href="https://www.fortiguard.com/psirt">https://www.fortiguard.com/psirt</a>                                                                                                                                                                                                                  |
| IBM                    | Security bulletins, <a href="https://cloud.ibm.com/status/security">https://cloud.ibm.com/status/security</a><br>Research, Collaborate and Act on threat intelligence, <a href="https://exchange.xforce.ibmcloud.com/">https://exchange.xforce.ibmcloud.com/</a>                                                    |
| MS Windows             | The Microsoft Security Response Center (MSRC), <a href="https://msrc.microsoft.com/update-guide/">https://msrc.microsoft.com/update-guide/</a>                                                                                                                                                                      |
| SAP                    | SAP Security Notes, <a href="https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html">https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html</a>                                                                                                                       |
| Dell                   | Security Advisories, Notices and Resources, <a href="https://www.dell.com/support/security/en-us">https://www.dell.com/support/security/en-us</a>                                                                                                                                                                   |
| HPE                    | HPE Security Bulletin Library, <a href="https://support.hpe.com/connect/s/securitybulletinlibrary">https://support.hpe.com/connect/s/securitybulletinlibrary</a><br>Security Bulletins, <a href="https://support.hp.com/us-en/security-bulletins">https://support.hp.com/us-en/security-bulletins</a>               |
| Cisco                  | Cisco Security Advisories, <a href="https://sec.cloudapps.cisco.com/security/center/publicationListing.x">https://sec.cloudapps.cisco.com/security/center/publicationListing.x</a>                                                                                                                                  |
| Palo Alto              | Palo Alto Networks Security Advisories, <a href="https://security.paloaltonetworks.com/">https://security.paloaltonetworks.com/</a>                                                                                                                                                                                 |
| Ivanti                 | Security Advisory, <a href="https://www.ivanti.com/blog/topics/security-advisory">https://www.ivanti.com/blog/topics/security-advisory</a>                                                                                                                                                                          |
| Mozilla                | Mozilla Foundation Security Advisories, <a href="https://www.mozilla.org/en-US/security/advisories/">https://www.mozilla.org/en-US/security/advisories/</a>                                                                                                                                                         |
| Android                | Android Security Bulletins, <a href="https://source.android.com/docs/security/bulletin/asb-overview">https://source.android.com/docs/security/bulletin/asb-overview</a>                                                                                                                                             |
| Zyxel                  | Security Advisories, <a href="https://www.zyxel.com/global/en/support/security-advisories">https://www.zyxel.com/global/en/support/security-advisories</a>                                                                                                                                                          |
| D-Link                 | Global Security Advisories, Responses, and Notices, <a href="https://supportannouncement.us.dlink.com/">https://supportannouncement.us.dlink.com/</a>                                                                                                                                                               |
| Adobe                  | Security Bulletins and Advisories, <a href="https://helpx.adobe.com/security/security-bulletin.html">https://helpx.adobe.com/security/security-bulletin.html</a>                                                                                                                                                    |
| Siemens                | Siemens ProductCERT and Siemens CERT, <a href="https://www.siemens.com/global/en/products/services/cert.html">https://www.siemens.com/global/en/products/services/cert.html</a>                                                                                                                                     |
| Splunk                 | Splunk Security Advisories, <a href="https://advisory.splunk.com/">https://advisory.splunk.com/</a>                                                                                                                                                                                                                 |