

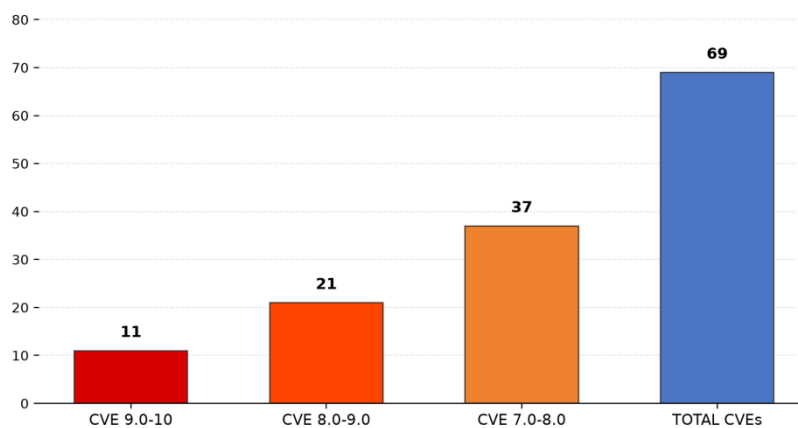


Newsletter on system vulnerabilities and  
cybersecurity news.

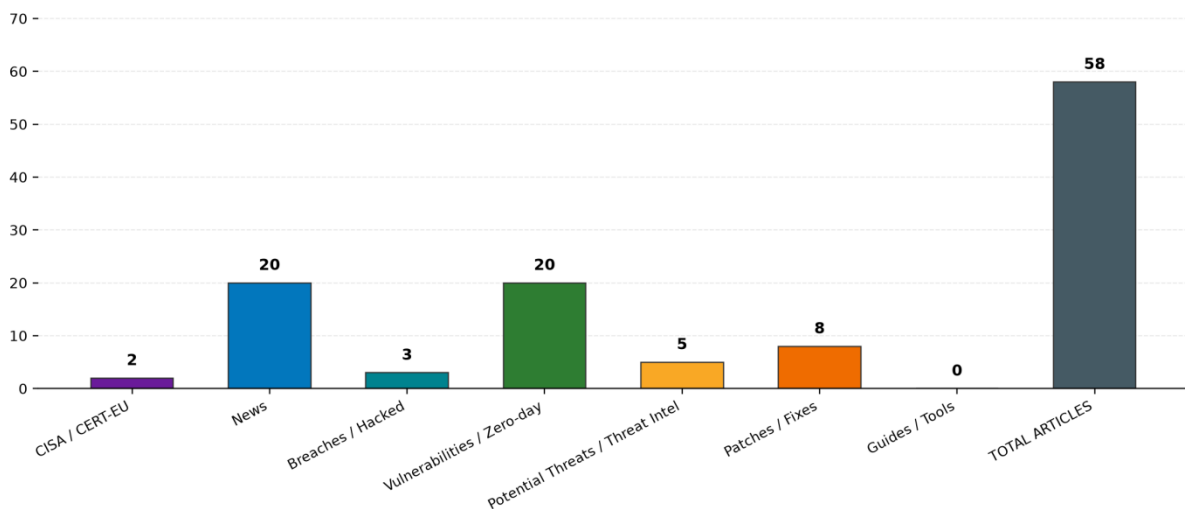
National Cyber Security Authority (NCSA)

Date: 26/09/2026 - 29/09/2026

**# of CVEs per CVSS score**



**# of articles per section**



## Contents

|                                                             |    |
|-------------------------------------------------------------|----|
| Common Vulnerabilities and Exposures (CVEs) .....           | 3  |
| CISA/CERT-EU Alerts & Advisories.....                       | 10 |
| News.....                                                   | 11 |
| Breaches / Compromised / Hacked.....                        | 12 |
| Vulnerabilities / Flaws / Zero-day.....                     | 12 |
| Patches / Updates / Fixes .....                             | 13 |
| Potential threats / Threat intelligence .....               | 14 |
| Guides / Tools.....                                         | 14 |
| References.....                                             | 15 |
| Annex – Websites with vendor specific vulnerabilities ..... | 16 |

## 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-2026-102240</a> | 10,0      | Netcore NAP930                                                             | Improper Neutralization of Special Elements used in a Command ('Command Injection'); Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')         | 0.1.241010.141410                                                                                        | <a href="https://github.com/senxitoyshuyi/HACKALL/blob/main/netcore_NAP930%20V0.1.241010.141410%20Router/NAP930_network_tools_command_injection.md">https://github.com/senxitoyshuyi/HACKALL/blob/main/netcore_NAP930%20V0.1.241010.141410%20Router/NAP930_network_tools_command_injection.md</a><br><a href="https://vuldb.com/cve/CVE-2026-102240">https://vuldb.com/cve/CVE-2026-102240</a><br><a href="https://vuldb.com/submit/931247">https://vuldb.com/submit/931247</a><br><a href="https://vuldb.com/vuln/411139">https://vuldb.com/vuln/411139</a><br><a href="https://vuldb.com/vuln/411139/cti">https://vuldb.com/vuln/411139/cti</a>                                                                                       |              |             |                  |
| <a href="#">CVE-2026-88773</a>  | 10,0      | Citrix NetScaler ADC and Citrix NetScaler Gateway                          | Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')                                                                                                        | before 14.1-73.37; before 13.1-64.23; before 13.1-37.279; before 13.1-64.23.                             | <a href="https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096">https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |              |             |                  |
| <a href="#">CVE-2026-100741</a> | 9,8       | the JScript event-script dispatcher in Progressive Robot Ltd's hMailServer | Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')                                                                                                  | versions 6.0.0 through 6.3.3; Before 6.2.25                                                              | <a href="https://gitlab.com/Progressiverobot/hmailserver/-/commit/5a3de9001d6c5e833662ada8e44ce10d42d76b1a">https://gitlab.com/Progressiverobot/hmailserver/-/commit/5a3de9001d6c5e833662ada8e44ce10d42d76b1a</a><br><a href="https://gitlab.com/Progressiverobot/hmailserver/-/releases/v6.3.4">https://gitlab.com/Progressiverobot/hmailserver/-/releases/v6.3.4</a>                                                                                                                                                                                                                                                                                                                                                                  | none         | yes         | total            |
| <a href="#">CVE-2026-101354</a> | 9,6       | FAST FAC1203R                                                              | Improper Restriction of Operations within the Bounds of a Memory Buffer; Stack-based Buffer Overflow                                                                                    | 20200116_2.0.4                                                                                           | <a href="https://github.com/xiaobor123/vuls-find-VxWorks/tree/main/vul-find-FAST_FAC1203R-twlantask-MmtAtePrase-stack-overflow(1)/vul-find-FAST_FAC1203R-twlantask-MmtAtePrase-stack-overflow">https://github.com/xiaobor123/vuls-find-VxWorks/tree/main/vul-find-FAST_FAC1203R-twlantask-MmtAtePrase-stack-overflow(1)/vul-find-FAST_FAC1203R-twlantask-MmtAtePrase-stack-overflow</a><br><a href="https://vuldb.com/cve/CVE-2026-101354">https://vuldb.com/cve/CVE-2026-101354</a><br><a href="https://vuldb.com/submit/927238">https://vuldb.com/submit/927238</a><br><a href="https://vuldb.com/vuln/411088">https://vuldb.com/vuln/411088</a><br><a href="https://vuldb.com/vuln/411088/cti">https://vuldb.com/vuln/411088/cti</a> |              |             |                  |
| <a href="#">CVE-2026-12342</a>  | 9,6       | IdentityIQ                                                                 | Improper Input Validation                                                                                                                                                               | 8.5 through 8.5p2; 8.4 through 8.4p4; 8.3 through 8.3p5                                                  | <a href="https://www.sailpoint.com/security-advisories/">https://www.sailpoint.com/security-advisories/</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | none         | no          | total            |
| <a href="#">CVE-2026-88804</a>  | 9,6       | Rancher                                                                    | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')                                                                                                    | before 2.15.2, 2.14; before 2.14.6, 2.13; before 2.13.10, 2.12; before 2.12.14 and 2.11; before 2.11.18. | <a href="https://github.com/rancher/rancher/security/advisories/GHSA-992f-xh8r-jq2f">https://github.com/rancher/rancher/security/advisories/GHSA-992f-xh8r-jq2f</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | none         | no          | total            |
| <a href="#">CVE-2026-101187</a> | 9,1       | Ziroom ZHOME A0101                                                         | Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in a Command ('Command Injection') | 1.0.1.0                                                                                                  | <a href="https://github.com/Wl1z1112/ZHOME_A0101/blob/main/pop_usb_device_path_command_injection.md">https://github.com/Wl1z1112/ZHOME_A0101/blob/main/pop_usb_device_path_command_injection.md</a><br><a href="https://vuldb.com/cve/CVE-2026-101187">https://vuldb.com/cve/CVE-2026-101187</a><br><a href="https://vuldb.com/submit/906506">https://vuldb.com/submit/906506</a><br><a href="https://vuldb.com/vuln/411008">https://vuldb.com/vuln/411008</a><br><a href="https://vuldb.com/vuln/411008/cti">https://vuldb.com/vuln/411008/cti</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-2026-101894</a> | 9,1       | decompress                        | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); Improper Link Resolution Before File Access ('Link Following') | Prior to 10.2.2 and 11.1.4; through 4.2.1.   | <a href="https://github.com/XhmikosR/decompress/commit/5f4b2f64abb31bba11ef8975b595f7df2558d8">https://github.com/XhmikosR/decompress/commit/5f4b2f64abb31bba11ef8975b595f7df2558d8</a><br><a href="https://github.com/XhmikosR/decompress/commit/f6c88c668216d6a12c6cec4fe0b6c70bf77050a">https://github.com/XhmikosR/decompress/commit/f6c88c668216d6a12c6cec4fe0b6c70bf77050a</a><br><a href="https://github.com/XhmikosR/decompress/releases/tag/v10.2.2">https://github.com/XhmikosR/decompress/releases/tag/v10.2.2</a><br><a href="https://github.com/XhmikosR/decompress/releases/tag/v11.1.4">https://github.com/XhmikosR/decompress/releases/tag/v11.1.4</a><br><a href="https://github.com/XhmikosR/decompress/security/advisories/GHSA-hrh2-vp3x-79xf">https://github.com/XhmikosR/decompress/security/advisories/GHSA-hrh2-vp3x-79xf</a>                                                                                                                                          | none         | yes         | total            |
| <a href="#">CVE-2026-102268</a> | 9,1       | PyJWT                             | Improper Verification of Cryptographic Signature                                                                                               | Prior to 2.14.0                              | <a href="https://github.com/jpadilla/pyjwt/commit/8b4e233a22206b34ec1186e912e75c0b2396ac07">https://github.com/jpadilla/pyjwt/commit/8b4e233a22206b34ec1186e912e75c0b2396ac07</a><br><a href="https://github.com/jpadilla/pyjwt/releases/tag/2.14.0">https://github.com/jpadilla/pyjwt/releases/tag/2.14.0</a><br><a href="https://github.com/jpadilla/pyjwt/security/advisories/GHSA-fic3-869f-ixw9">https://github.com/jpadilla/pyjwt/security/advisories/GHSA-fic3-869f-ixw9</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |              |             |                  |
| <a href="#">CVE-2026-102361</a> | 9,1       | mall4j                            | Missing Authentication for Critical Function                                                                                                   | through 4.0                                  | <a href="https://github.com/LinYuanyi/cve-request-poc/blob/114b3f0d149e50a7678f591bf8043399fc9ac96c/mall4j/A01_updatepwd_account_takeover.py">https://github.com/LinYuanyi/cve-request-poc/blob/114b3f0d149e50a7678f591bf8043399fc9ac96c/mall4j/A01_updatepwd_account_takeover.py</a><br><a href="https://github.com/qz-vami/mall4j">https://github.com/qz-vami/mall4j</a><br><a href="https://github.com/qz-vami/mall4j/blob/ffc672fc1aa4320ce02d0b93853bb456ae0a4dae/vami-shop-api/src/main/java/com/vami/shop/api/controller/UserRegisterController.java#L78-L100">https://github.com/qz-vami/mall4j/blob/ffc672fc1aa4320ce02d0b93853bb456ae0a4dae/vami-shop-api/src/main/java/com/vami/shop/api/controller/UserRegisterController.java#L78-L100</a><br><a href="https://www.vulncheck.com/advisories/mall4j-through-4.0-missing-authentication-in-password-update-endpoint">https://www.vulncheck.com/advisories/mall4j-through-4.0-missing-authentication-in-password-update-endpoint</a> |              |             |                  |
| <a href="#">CVE-2026-49994</a>  | 9,1       | bluehood                          | Missing Authentication for Critical Function; Missing Authorization                                                                            | Prior to version 0.7.1                       | <a href="https://github.com/dannymcc/bluehood/commit/401479938c0deb1f6f6847d442f98a2d03efca68">https://github.com/dannymcc/bluehood/commit/401479938c0deb1f6f6847d442f98a2d03efca68</a><br><a href="https://github.com/dannymcc/bluehood/releases/tag/v0.7.1">https://github.com/dannymcc/bluehood/releases/tag/v0.7.1</a><br><a href="https://github.com/dannymcc/bluehood/security/advisories/GHSA-qj2l-wcq3-74jw">https://github.com/dannymcc/bluehood/security/advisories/GHSA-qj2l-wcq3-74jw</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | none         | yes         | total            |
| <a href="#">CVE-2026-100520</a> | 8,8       | Laranode versions                 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')                                                                 | versions before 1.2.1                        | <a href="https://github.com/crivation/laranode">https://github.com/crivation/laranode</a><br><a href="https://github.com/crivation/laranode/blob/v1.2/app/Actions/Filemanager/UploadFileAction.php">https://github.com/crivation/laranode/blob/v1.2/app/Actions/Filemanager/UploadFileAction.php</a><br><a href="https://github.com/crivation/laranode/commit/5c2b18ae99caf77a6fb6cc5c0ab66562bd673424">https://github.com/crivation/laranode/commit/5c2b18ae99caf77a6fb6cc5c0ab66562bd673424</a><br><a href="https://github.com/crivation/laranode/pull/21">https://github.com/crivation/laranode/pull/21</a><br><a href="https://github.com/crivation/laranode/releases/tag/v1.2.1">https://github.com/crivation/laranode/releases/tag/v1.2.1</a><br><a href="https://github.com/crivation/laranode/security/advisories/GHSA-34h2-2696-vfvr">https://github.com/crivation/laranode/security/advisories/GHSA-34h2-2696-vfvr</a>                                                               |              |             |                  |
| <a href="#">CVE-2026-101860</a> | 8,8       | RaspAP raspap-webgui              | Incorrect Privilege Assignment; Improper Privilege Management                                                                                  | up to 3.5.5.                                 | <a href="https://gist.github.com/simvat/10422042d6d5225b2heb97754de4b68c">https://gist.github.com/simvat/10422042d6d5225b2heb97754de4b68c</a><br><a href="https://vuldb.com/cve/CVE-2026-101860">https://vuldb.com/cve/CVE-2026-101860</a><br><a href="https://vuldb.com/submit/930259">https://vuldb.com/submit/930259</a><br><a href="https://vuldb.com/vuln/411094">https://vuldb.com/vuln/411094</a><br><a href="https://vuldb.com/vuln/411094/ctj">https://vuldb.com/vuln/411094/ctj</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |              |             |                  |
| <a href="#">CVE-2026-12264</a>  | 8,8       | Zohocorp ManageEngine DDI Central | Unrestricted Upload of File with Dangerous Type                                                                                                | versions before 6201                         | <a href="https://www.manageengine.com/dns-dhcp-ipam/security-updates/security-updates.html">https://www.manageengine.com/dns-dhcp-ipam/security-updates/security-updates.html</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | none         | no          | total            |
| <a href="#">CVE-2026-12268</a>  | 8,8       | ManageEngine DDI Central          | Improper Input Validation                                                                                                                      | prior to 6201                                | <a href="https://www.manageengine.com/dns-dhcp-ipam/security-updates/security-updates.html">https://www.manageengine.com/dns-dhcp-ipam/security-updates/security-updates.html</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | none         | no          | total            |
| <a href="#">CVE-2026-12269</a>  | 8,8       | Zohocorp ManageEngine DDI Central | Improper Privilege Management; Unrestricted Upload of File with Dangerous Type                                                                 | prior to 6201                                | <a href="https://www.manageengine.com/dns-dhcp-ipam/security-updates/cve-2026-12269.html">https://www.manageengine.com/dns-dhcp-ipam/security-updates/cve-2026-12269.html</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | none         | no          | total            |
| <a href="#">CVE-2026-78424</a>  | 8,8       | NeuVector                         | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')                                                     | 5; before 5.4.11; before 5.5.4; before 5.6.2 | <a href="https://github.com/neuvector/neuvector/security/advisories/GHSA-vr77-8vmq-qfml">https://github.com/neuvector/neuvector/security/advisories/GHSA-vr77-8vmq-qfml</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | none         | no          | total            |

| 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-2024-42002</a>  | 8,4       | the Robot Operating System       | Improper Control of Generation of Code ('Code Injection'); Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') | Rolling Ridley; Lyrical Luth; Kilted Kaiju; Jazzy Jalisco; Iron Irwini; Humble Hawksbill; Galactic Geochelone; Foxy Fitzroy; Eloquent Elusor; Dashing Diademata; Crystal Clemmys | <a href="https://github.com/ros2/ros2cli/pull/1001">https://github.com/ros2/ros2cli/pull/1001</a><br><a href="https://github.com/ros2/ros2cli/pull/133#discussion_r223081766">https://github.com/ros2/ros2cli/pull/133#discussion_r223081766</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |              |             |                  |
| <a href="#">CVE-2026-100369</a> | 8,4       | CliIvoke; AlastairLundy.CliIvoke | Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')                                                                | versions 2.0.0 through 2.8.4; 2.9.0 through 2.9.3; 2.10.0 through 2.10.4; 3.0.0-alpha.1 through 3.0.0-beta.1; versions 2.0.0-alpha.1 through 2.0.0                               | <a href="https://github.com/alastairlundy/CliIvoke/security/advisories/GHSA-i73w-8hfr-4qc9">https://github.com/alastairlundy/CliIvoke/security/advisories/GHSA-i73w-8hfr-4qc9</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | none         | no          | total            |
| <a href="#">CVE-2026-55157</a>  | 8,4       | token-optimizer-mcp              | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')                                                        | Prior to version 5.1.0                                                                                                                                                           | <a href="https://github.com/ooptes/token-optimizer-mcp/commit/b4ee96dac799cbfa0a9f9c17844ce9d613cbcc7">https://github.com/ooptes/token-optimizer-mcp/commit/b4ee96dac799cbfa0a9f9c17844ce9d613cbcc7</a><br><a href="https://github.com/ooptes/token-optimizer-mcp/releases/tag/v5.1.0">https://github.com/ooptes/token-optimizer-mcp/releases/tag/v5.1.0</a><br><a href="https://github.com/ooptes/token-optimizer-mcp/security/advisories/GHSA-49mq-fc6q-3h46">https://github.com/ooptes/token-optimizer-mcp/security/advisories/GHSA-49mq-fc6q-3h46</a>                                                                                                                                                                                                                                                  |              |             |                  |
| <a href="#">CVE-2026-101188</a> | 8,3       | Netcore POWER13                  | Weak Password Recovery Mechanism for Forgotten Password                                                                                           | 2.0.240730.162638                                                                                                                                                                | <a href="https://github.com/I22Heart/cve_report/blob/main/Netcore%20POWER13%20Unauthenticated%20routerd%20passwd%20set%20Password%20Reset%20Vulnerability.md">https://github.com/I22Heart/cve_report/blob/main/Netcore POWER13 Unauthenticated routerd passwd set Password Reset Vulnerability.md</a><br><a href="https://vuln.db.com/cve/CVE-2026-101188">https://vuln.db.com/cve/CVE-2026-101188</a><br><a href="https://vuln.db.com/submit/906532">https://vuln.db.com/submit/906532</a><br><a href="https://vuln.db.com/vuln/411009">https://vuln.db.com/vuln/411009</a><br><a href="https://vuln.db.com/vuln/411009/ctj">https://vuln.db.com/vuln/411009/ctj</a>                                                                                                                                      |              |             |                  |
| <a href="#">CVE-2026-100391</a> | 8,2       | MediaFlow Proxy                  | Server-Side Request Forgery (SSRF)                                                                                                                | through 2.4.9                                                                                                                                                                    | <a href="https://github.com/mhdzumair/mediaflow-proxy">https://github.com/mhdzumair/mediaflow-proxy</a><br><a href="https://github.com/mhdzumair/mediaflow-proxy/blob/2.4.9/mediaflow_proxy/routes/proxy.py#L532-L569">https://github.com/mhdzumair/mediaflow-proxy/blob/2.4.9/mediaflow_proxy/routes/proxy.py#L532-L569</a><br><a href="https://github.com/mhdzumair/mediaflow-proxy/commit/99f4af1153d4766420a098a232183cba1efdc560">https://github.com/mhdzumair/mediaflow-proxy/commit/99f4af1153d4766420a098a232183cba1efdc560</a><br><a href="https://www.vulncheck.com/advisories/mediaflow-proxy-through-2.4.9-server-side-request-forgery-via-incomplete-validation">https://www.vulncheck.com/advisories/mediaflow-proxy-through-2.4.9-server-side-request-forgery-via-incomplete-validation</a> |              |             |                  |
| <a href="#">CVE-2026-100833</a> | 8,2       | Contrast (edgelessys/contrast)   | Improper Input Validation                                                                                                                         | before 1.23.1                                                                                                                                                                    | <a href="https://github.com/edgelessys/contrast/security/advisories/GHSA-m2qq-wrxv-h898">https://github.com/edgelessys/contrast/security/advisories/GHSA-m2qq-wrxv-h898</a><br><a href="https://www.vulncheck.com/advisories/contrast-before-1.23.1-image-substitution-via-policy-generation">https://www.vulncheck.com/advisories/contrast-before-1.23.1-image-substitution-via-policy-generation</a>                                                                                                                                                                                                                                                                                                                                                                                                     | none         | no          | total            |
| <a href="#">CVE-2026-101060</a> | 8,2       | python-utcp versions             | Server-Side Request Forgery (SSRF)                                                                                                                | versions before 1.1.4                                                                                                                                                            | <a href="https://github.com/universal-tool-calling-protocol/python-utcp/security/advisories/GHSA-9ghq-99ww-9mqc">https://github.com/universal-tool-calling-protocol/python-utcp/security/advisories/GHSA-9ghq-99ww-9mqc</a><br><a href="https://www.vulncheck.com/advisories/python-utcp-before-1.1.4-ssrf-via-unvalidated-http-redirects">https://www.vulncheck.com/advisories/python-utcp-before-1.1.4-ssrf-via-unvalidated-http-redirects</a>                                                                                                                                                                                                                                                                                                                                                           | poc          | no          | partial          |
| <a href="#">CVE-2026-101292</a> | 8,2       | Apache ActiveMQ Artemis          | Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')                                                                | before 2.34.0                                                                                                                                                                    | <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-2026-101292">https://access.redhat.com/security/cve/CVE-2026-101292</a><br><a href="https://bugzilla.redhat.com/show_bug.cgi?id=2482963">https://bugzilla.redhat.com/show_bug.cgi?id=2482963</a>                                                                                                                                                                                                                                                                                                                                                                                                                                    | none         | yes         | partial          |
| <a href="#">CVE-2026-54160</a>  | 8,2       | Network UPS Tools                | Inclusion of Functionality from Untrusted Control Sphere                                                                                          | < 658b24ef8410648ceca6d5a59e8690efbc8c36bc                                                                                                                                       | <a href="https://github.com/networkupstools/nut/commit/658b24ef8410648ceca6d5a59e8690efbc8c36bc">https://github.com/networkupstools/nut/commit/658b24ef8410648ceca6d5a59e8690efbc8c36bc</a><br><a href="https://github.com/networkupstools/nut/security/advisories/GHSA-w6wj-3r73-fxmh">https://github.com/networkupstools/nut/security/advisories/GHSA-w6wj-3r73-fxmh</a>                                                                                                                                                                                                                                                                                                                                                                                                                                 | none         | no          | total            |

| 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-2026-100387</a> | 8,1       | pgPointcloud               | Out-of-bounds Read                                                                         | through 1.2.5                                                             | <a href="https://github.com/pgpointcloud/pointcloud">https://github.com/pgpointcloud/pointcloud</a><br><a href="https://github.com/pgpointcloud/pointcloud/blob/v1.2.5/lib/pc_bytes.c#L1347-L1373">https://github.com/pgpointcloud/pointcloud/blob/v1.2.5/lib/pc_bytes.c#L1347-L1373</a><br><a href="https://github.com/pgpointcloud/pointcloud/issues/387">https://github.com/pgpointcloud/pointcloud/issues/387</a><br><a href="https://github.com/pgpointcloud/pointcloud/pull/388">https://github.com/pgpointcloud/pointcloud/pull/388</a><br><a href="https://www.vulncheck.com/advisories/pgpointcloud-through-1.2.5-heap-out-of-bounds-read-via-wkb-deserialization">https://www.vulncheck.com/advisories/pgpointcloud-through-1.2.5-heap-out-of-bounds-read-via-wkb-deserialization</a> |              |             |                  |
| <a href="#">CVE-2026-100389</a> | 8,1       | GestSup versions           | Unrestricted Upload of File with Dangerous Type                                            | versions before 3.2.61                                                    | <a href="https://gestsup.fr/index.php?page=changelog">https://gestsup.fr/index.php?page=changelog</a><br><a href="https://gestsup.fr/index.php?page=download">https://gestsup.fr/index.php?page=download</a><br><a href="https://www.vulncheck.com/advisories/gestsup-before-3.2.61-remote-code-execution-via-imap-attachment">https://www.vulncheck.com/advisories/gestsup-before-3.2.61-remote-code-execution-via-imap-attachment</a>                                                                                                                                                                                                                                                                                                                                                         |              |             |                  |
| <a href="#">CVE-2026-102422</a> | 8,1       | shell-quote                | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 1.8.4 prior to 1.11.0                                                     | <a href="https://github.com/ljharb/shell-quote">https://github.com/ljharb/shell-quote</a><br><a href="https://github.com/ljharb/shell-quote/commit/6002b2ed90c6b83095eb272b6b0adaf3a172b0bc">https://github.com/ljharb/shell-quote/commit/6002b2ed90c6b83095eb272b6b0adaf3a172b0bc</a><br><a href="https://github.com/ljharb/shell-quote/security/advisories/GHSA-pqq4-i6r4-53mv">https://github.com/ljharb/shell-quote/security/advisories/GHSA-pqq4-i6r4-53mv</a><br><a href="https://www.npmjs.com/package/shell-quote">https://www.npmjs.com/package/shell-quote</a>                                                                                                                                                                                                                        |              |             |                  |
| <a href="#">CVE-2026-93348</a>  | 8,1       | Unslloth Zoo               | Improper Control of Generation of Code ('Code Injection')                                  | before 2026.8.14; 2025.9.9 through 2026.8.19                              | <a href="https://github.com/unsllothai/unslloth-zoo/pull/1083">https://github.com/unsllothai/unslloth-zoo/pull/1083</a><br><a href="https://github.com/unsllothai/unslloth-zoo/pull/1108">https://github.com/unsllothai/unslloth-zoo/pull/1108</a><br><a href="https://github.com/unsllothai/unslloth/commit/92ee0207a38ebc8af1a0e678aa92d7e7d901ea0d">https://github.com/unsllothai/unslloth/commit/92ee0207a38ebc8af1a0e678aa92d7e7d901ea0d</a><br><a href="https://www.vulncheck.com/advisories/unslloth-zoo-code-injection-via-model-type-in-config-ison">https://www.vulncheck.com/advisories/unslloth-zoo-code-injection-via-model-type-in-config-ison</a>                                                                                                                                |              |             |                  |
| <a href="#">CVE-2026-93355</a>  | 8,1       | LiteLLM                    | Weak Authentication                                                                        | 1.102.1 and earlier; f4308bc124eebc783dfc51790ce8db27ed21ae00 and earlier | <a href="https://www.ox.security/blog/litellm-an-ordinary-login-token-can-become-someone-elses-admin-account/">https://www.ox.security/blog/litellm-an-ordinary-login-token-can-become-someone-elses-admin-account/</a><br><a href="https://www.vulncheck.com/advisories/litellm-weak-jwt-authentication-via-email-based-user-lookup">https://www.vulncheck.com/advisories/litellm-weak-jwt-authentication-via-email-based-user-lookup</a>                                                                                                                                                                                                                                                                                                                                                      |              |             |                  |
| <a href="#">CVE-2026-101045</a> | 8,0       | fleet                      | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | before 2026-08-19                                                         | <a href="https://github.com/fleetdm/fleet/security/advisories/GHSA-fv3p-h7wv-2jgm">https://github.com/fleetdm/fleet/security/advisories/GHSA-fv3p-h7wv-2jgm</a><br><a href="https://www.vulncheck.com/advisories/fleet-homebrew-cask-os-command-injection-via-metadata">https://www.vulncheck.com/advisories/fleet-homebrew-cask-os-command-injection-via-metadata</a>                                                                                                                                                                                                                                                                                                                                                                                                                          | none         | no          | total            |
| <a href="#">CVE-2026-16513</a>  | 7,8       | subsys/rtio/rtio_sys calls | Out-of-bounds Write                                                                        | before v4.3.0)                                                            | <a href="https://github.com/zephyrproject-rtos/zephyr/commit/95c355c425763f5e735b9ef54dacce2c4ce21f">https://github.com/zephyrproject-rtos/zephyr/commit/95c355c425763f5e735b9ef54dacce2c4ce21f</a><br><a href="https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-fwmc-q8gq-icxq">https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-fwmc-q8gq-icxq</a>                                                                                                                                                                                                                                                                                                                                                                                                  |              |             |                  |
| <a href="#">CVE-2026-18413</a>  | 7,8       | zephyr                     | Out-of-bounds Write                                                                        | 2.5.0 prior to 4.4.2                                                      | <a href="https://github.com/zephyrproject-rtos/zephyr/commit/3bda971a52ddb9ec28f6f3b006d34e8b9e5a9">https://github.com/zephyrproject-rtos/zephyr/commit/3bda971a52ddb9ec28f6f3b006d34e8b9e5a9</a><br><a href="https://github.com/zephyrproject-rtos/zephyr/commit/9338c518bf2b6a396f166d4dbe9985ce7e44379c">https://github.com/zephyrproject-rtos/zephyr/commit/9338c518bf2b6a396f166d4dbe9985ce7e44379c</a><br><a href="https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-7iqg-2q5q-hcrp">https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-7iqg-2q5q-hcrp</a><br><a href="https://pentraze.com/vulnerability-reports">https://pentraze.com/vulnerability-reports</a>                                                                                  |              |             |                  |
| <a href="#">CVE-2026-4556</a>   | 7,8       | Exam4; the com             | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 25.12.28.0 and earlier                                                    | <a href="https://pentraze.com/vulnerability-reports">https://pentraze.com/vulnerability-reports</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | none         | no          | total            |
| <a href="#">CVE-2026-100704</a> | 7,7       | Kyverno                    | Incorrect Authorization                                                                    | In versions 1.14.0 through 1.19.0                                         | <a href="https://github.com/kyverno/kyverno/security/advisories/GHSA-5c4f-wwfq-pj4c">https://github.com/kyverno/kyverno/security/advisories/GHSA-5c4f-wwfq-pj4c</a><br><a href="https://www.vulncheck.com/advisories/kyverno-before-1.19.1-imagevalidatingpolicy-exception-bypass">https://www.vulncheck.com/advisories/kyverno-before-1.19.1-imagevalidatingpolicy-exception-bypass</a>                                                                                                                                                                                                                                                                                                                                                                                                        | poc          | no          | partial          |
| <a href="#">CVE-2026-86158</a>  | 7,7       | the local                  | Missing Authentication for Critical Function                                               | 1.0.0 prior to 8.2.0                                                      | <a href="https://www.telerik.com/fiddler/fiddler-everywhere/documentation/knowledge-base/kb-security-exposed-dangerous-method-or-function-cve-2026-aaaaa">https://www.telerik.com/fiddler/fiddler-everywhere/documentation/knowledge-base/kb-security-exposed-dangerous-method-or-function-cve-2026-aaaaa</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-2026-55160</a>  | 7,6       | Stringer         | Server-Side Request Forgery (SSRF)                              | < 75cb0955919a362ac49d23c8a14892d0f59ea1c4        | <a href="https://github.com/stringer-rss/stringer/commit/75cb0955919a362ac49d23c8a14892d0f59ea1c4">https://github.com/stringer-rss/stringer/commit/75cb0955919a362ac49d23c8a14892d0f59ea1c4</a><br><a href="https://github.com/stringer-rss/stringer/pull/1548">https://github.com/stringer-rss/stringer/pull/1548</a><br><a href="https://github.com/stringer-rss/stringer/security/advisories/GHSA-496x-437q-h35g">https://github.com/stringer-rss/stringer/security/advisories/GHSA-496x-437q-h35g</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | poc          | no          | partial          |
| <a href="#">CVE-2026-100631</a> | 7,5       | Parse Server     | Improper Neutralization of Special Elements in Data Query Logic | versions prior to 8.6.90; prior to 9.10.1-alpha.9 | <a href="https://github.com/parse-community/parse-server/security/advisories/GHSA-cc6h-c8m4-hgrx">https://github.com/parse-community/parse-server/security/advisories/GHSA-cc6h-c8m4-hgrx</a><br><a href="https://www.vulncheck.com/advisories/parse-server-9.0.0-unauthenticated-installation-deletion-via-operator-injection">https://www.vulncheck.com/advisories/parse-server-9.0.0-unauthenticated-installation-deletion-via-operator-injection</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | none         | yes         | partial          |
| <a href="#">CVE-2026-100700</a> | 7,5       | nodemailer       | Inefficient Algorithmic Complexity                              | before 10.0.6                                     | <a href="https://github.com/nodemailer/nodemailer/security/advisories/GHSA-v53p-9fqp-m79j">https://github.com/nodemailer/nodemailer/security/advisories/GHSA-v53p-9fqp-m79j</a><br><a href="https://www.vulncheck.com/advisories/nodemailer-before-10.0.6-denial-of-service-via-addressparser">https://www.vulncheck.com/advisories/nodemailer-before-10.0.6-denial-of-service-via-addressparser</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | poc          | yes         | partial          |
| <a href="#">CVE-2026-101878</a> | 7,5       | bitwarden server | Incorrect Implementation of Authentication Algorithm            | before 2026.5.0                                   | <a href="https://github.com/bitwarden/server/commit/27ae3d5455f723975fac03819eae8a8710666bc4">https://github.com/bitwarden/server/commit/27ae3d5455f723975fac03819eae8a8710666bc4</a><br><a href="https://github.com/bitwarden/server/pull/7501">https://github.com/bitwarden/server/pull/7501</a><br><a href="https://github.com/bitwarden/server/releases/tag/v2026.5.0">https://github.com/bitwarden/server/releases/tag/v2026.5.0</a><br><a href="https://sanjokkarki.com.np/blog/bitwarden-sso-externalid-truncation">https://sanjokkarki.com.np/blog/bitwarden-sso-externalid-truncation</a><br><a href="https://www.vulncheck.com/advisories/bitwarden-server-authentication-bypass-via-sso-identifier-truncation">https://www.vulncheck.com/advisories/bitwarden-server-authentication-bypass-via-sso-identifier-truncation</a>                                                                                                                                                                                                                       |              |             |                  |
| <a href="#">CVE-2026-102276</a> | 7,5       | brace-expansion  | Uncontrolled Resource Consumption; Uncontrolled Recursion       | Prior to 1.1.19, 2.1.5, 3.0.7                     | <a href="https://github.com/juliangruber/brace-expansion/commit/0bcbfc0a5928c3073d48f42999d1ce4fc1c42fbc">https://github.com/juliangruber/brace-expansion/commit/0bcbfc0a5928c3073d48f42999d1ce4fc1c42fbc</a><br><a href="https://github.com/juliangruber/brace-expansion/commit/316359e6019c39b3254c8ba8e25dc586a480652c">https://github.com/juliangruber/brace-expansion/commit/316359e6019c39b3254c8ba8e25dc586a480652c</a><br><a href="https://github.com/juliangruber/brace-expansion/commit/5171e681c0922b7ae8bfa9a331e309107be6edc">https://github.com/juliangruber/brace-expansion/commit/5171e681c0922b7ae8bfa9a331e309107be6edc</a><br><a href="https://github.com/juliangruber/brace-expansion/commit/6735c94873ca570bcd6a0690033bdd3126379d3">https://github.com/juliangruber/brace-expansion/commit/6735c94873ca570bcd6a0690033bdd3126379d3</a><br><a href="https://github.com/juliangruber/brace-expansion/security/advisories/GHSA-6j4f-fi2q-mc7p">https://github.com/juliangruber/brace-expansion/security/advisories/GHSA-6j4f-fi2q-mc7p</a> |              |             |                  |
| <a href="#">CVE-2026-102281</a> | 7,5       | Nest             | Uncaught Exception; Uncontrolled Recursion                      | Prior to 11.2.4 and 12.0.2                        | <a href="https://github.com/nestjs/nest/commit/aa97b5144d8df1ce700aac521eb86449a679d6f">https://github.com/nestjs/nest/commit/aa97b5144d8df1ce700aac521eb86449a679d6f</a><br><a href="https://github.com/nestjs/nest/commit/e9dcd4c7ac64361fbfe79461da85f5b3fc3e02da">https://github.com/nestjs/nest/commit/e9dcd4c7ac64361fbfe79461da85f5b3fc3e02da</a><br><a href="https://github.com/nestjs/nest/pull/17737">https://github.com/nestjs/nest/pull/17737</a><br><a href="https://github.com/nestjs/nest/releases/tag/v11.2.4">https://github.com/nestjs/nest/releases/tag/v11.2.4</a><br><a href="https://github.com/nestjs/nest/releases/tag/v12.0.2">https://github.com/nestjs/nest/releases/tag/v12.0.2</a><br><a href="https://github.com/nestjs/nest/security/advisories/GHSA-A-m8vh-jmq9-5r9q">https://github.com/nestjs/nest/security/advisories/GHSA-A-m8vh-jmq9-5r9q</a>                                                                                                                                                                            |              |             |                  |
| <a href="#">CVE-2026-10758</a>  | 7,5       | Esri LERC        | Integer Overflow or Wraparound                                  | versions 4.1.0 and earlier                        | <a href="https://github.com/Esri/lerc/security/advisories/GHSA-cw29-mw7w-pj37">https://github.com/Esri/lerc/security/advisories/GHSA-cw29-mw7w-pj37</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | none         | yes         | partial          |
| <a href="#">CVE-2026-57443</a>  | 7,5       | SCBE-AETHERMOORE | Missing Authentication for Critical Function                    | in version 4.0.2 and prior                        | <a href="https://github.com/sssdandavis/SCBE-AETHERMOORE/commit/ca833795e01eab060e92572e5f667c0c136b8c1e">https://github.com/sssdandavis/SCBE-AETHERMOORE/commit/ca833795e01eab060e92572e5f667c0c136b8c1e</a><br><a href="https://github.com/sssdandavis/SCBE-AETHERMOORE/commit/de7779b722c501dbcf4eae95dd51bb3984506fb1">https://github.com/sssdandavis/SCBE-AETHERMOORE/commit/de7779b722c501dbcf4eae95dd51bb3984506fb1</a><br><a href="https://github.com/sssdandavis/SCBE-AETHERMOORE/security/advisories/GHSA-q986-4x7x-qx39">https://github.com/sssdandavis/SCBE-AETHERMOORE/security/advisories/GHSA-q986-4x7x-qx39</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-2026-91765</a>  | 7,5       | the SOAP XML                                                                                                    | Uncontrolled Recursion                                                                                                                                                                  | 8.2.* prior to 8.2.34;<br>8.3.* prior to 8.3.35;<br>8.4.* prior to 8.4.26;<br>8.5.* prior to 8.5.11 | <a href="https://github.com/php/php-src/security/advisories/GHSA-rgrp-mwpx-f6rm">https://github.com/php/php-src/security/advisories/GHSA-rgrp-mwpx-f6rm</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | none         | yes         | partial          |
| <a href="#">CVE-2026-95104</a>  | 7,5       | BUFFALO Wi-Fi products                                                                                          | Stack-based Buffer Overflow                                                                                                                                                             | prior to Ver.2.55; prior to Ver.1.71                                                                | <a href="https://vn.jp/en/vu/JVNVU94863997/">https://vn.jp/en/vu/JVNVU94863997/</a><br><a href="https://www.buffalo.jp/news/detail/20260928-01.html">https://www.buffalo.jp/news/detail/20260928-01.html</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |              |             |                  |
| <a href="#">CVE-2026-96280</a>  | 7,5       | Red Hat Enterprise Linux 10; Red Hat Enterprise Linux 7; Red Hat Enterprise Linux 8; Red Hat Enterprise Linux 9 | Numeric Truncation Error                                                                                                                                                                |                                                                                                     | <a href="https://access.redhat.com/security/cve/CVE-2026-96280">https://access.redhat.com/security/cve/CVE-2026-96280</a><br><a href="https://bugzilla.redhat.com/show_bug.cgi?id=2539419">https://bugzilla.redhat.com/show_bug.cgi?id=2539419</a><br><a href="https://github.com/flatpak/flatpak/security/advisories/GHSA-ir92-2v97-wqvc">https://github.com/flatpak/flatpak/security/advisories/GHSA-ir92-2v97-wqvc</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |              |             |                  |
| <a href="#">CVE-2026-100390</a> | 7,4       | Zoraxy                                                                                                          | Authentication Bypass by Spoofing                                                                                                                                                       | versions 3.2.3 through 3.3.4                                                                        | <a href="https://github.com/tobychui/zoraxy">https://github.com/tobychui/zoraxy</a><br><a href="https://github.com/tobychui/zoraxy/blob/v3.3.4/src/mod/auth/sso/forward/uttl.go#L127-L142">https://github.com/tobychui/zoraxy/blob/v3.3.4/src/mod/auth/sso/forward/uttl.go#L127-L142</a><br><a href="https://github.com/tobychui/zoraxy/commit/56bb3e5ab83eae42a64203028d73a001d6096c4">https://github.com/tobychui/zoraxy/commit/56bb3e5ab83eae42a64203028d73a001d6096c4</a><br><a href="https://github.com/tobychui/zoraxy/pull/1264">https://github.com/tobychui/zoraxy/pull/1264</a><br><a href="https://www.vulncheck.com/advisories/zoraxy-3.2.3-through-3.3.4-client-ip-spoofing-via-x-forwarded-for-ip-v6">https://www.vulncheck.com/advisories/zoraxy-3.2.3-through-3.3.4-client-ip-spoofing-via-x-forwarded-for-ip-v6</a>                                                                                                                                                                                                                                                                                                                                                                    | none         | no          | total            |
| <a href="#">CVE-2026-101043</a> | 7,4       | pnpm                                                                                                            | Insertion of Sensitive Information Into Sent Data                                                                                                                                       | before 11.11.0 and 10.7.0; before 10.34.5                                                           | <a href="https://github.com/pnpm/pnpm/security/advisories/GHSA-vx52-2968-3vc6">https://github.com/pnpm/pnpm/security/advisories/GHSA-vx52-2968-3vc6</a><br><a href="https://www.vulncheck.com/advisories/pnpm-11.0.0-before-11.11.0-environment-variable-exfiltration-via-proxy-settings">https://www.vulncheck.com/advisories/pnpm-11.0.0-before-11.11.0-environment-variable-exfiltration-via-proxy-settings</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |              |             |                  |
| <a href="#">CVE-2026-101916</a> | 7,4       | @grpc/grpc-js; JavaScript, without a C++ addon                                                                  | Improper Certificate Validation                                                                                                                                                         | Prior to 1.13.6 and 1.14.5                                                                          | <a href="https://github.com/grpc/grpc-node/commit/2a84ec8b01b9db68ed9d2b117a53a81449edb8ee">https://github.com/grpc/grpc-node/commit/2a84ec8b01b9db68ed9d2b117a53a81449edb8ee</a><br><a href="https://github.com/grpc/grpc-node/commit/b4e0079c6d22a2adedfcac748e0bc083f783bc7c">https://github.com/grpc/grpc-node/commit/b4e0079c6d22a2adedfcac748e0bc083f783bc7c</a><br><a href="https://github.com/grpc/grpc-node/releases/tag/@grpc/grpc-js%401.14.5">https://github.com/grpc/grpc-node/releases/tag/@grpc/grpc-js%401.14.5</a><br><a href="https://github.com/grpc/grpc-node/security/advisories/GHSA-m9gg-hp2v-232j">https://github.com/grpc/grpc-node/security/advisories/GHSA-m9gg-hp2v-232j</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |              |             |                  |
| <a href="#">CVE-2026-102243</a> | 7,4       | MODSetter SurfSense                                                                                             | Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in a Command ('Command Injection') | up to 2.0.3.                                                                                        | <a href="https://gist.github.com/DReazer/81504d373f4e32206dc885d3c415e278">https://gist.github.com/DReazer/81504d373f4e32206dc885d3c415e278</a><br><a href="https://vuldb.com/cve/CVE-2026-102243">https://vuldb.com/cve/CVE-2026-102243</a><br><a href="https://vuldb.com/submit/933323">https://vuldb.com/submit/933323</a><br><a href="https://vuldb.com/vuln/411141">https://vuldb.com/vuln/411141</a><br><a href="https://vuldb.com/vuln/411141/ctj">https://vuldb.com/vuln/411141/ctj</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |              |             |                  |
| <a href="#">CVE-2026-102334</a> | 7,4       | Nginx Proxy Manager                                                                                             | Improper Restriction of Excessive Authentication Attempts                                                                                                                               | through 2.16.0                                                                                      | <a href="https://github.com/NginxProxyManager/nginx-proxy-manager">https://github.com/NginxProxyManager/nginx-proxy-manager</a><br><a href="https://github.com/NginxProxyManager/nginx-proxy-manager/blob/v2.16.0/backend/app.js#L15-L58">https://github.com/NginxProxyManager/nginx-proxy-manager/blob/v2.16.0/backend/app.js#L15-L58</a><br><a href="https://github.com/NginxProxyManager/nginx-proxy-manager/blob/v2.16.0/backend/internal/2fa.js#L196-L240">https://github.com/NginxProxyManager/nginx-proxy-manager/blob/v2.16.0/backend/internal/2fa.js#L196-L240</a><br><a href="https://github.com/NginxProxyManager/nginx-proxy-manager/blob/v2.16.0/backend/internal/token.js#L154-L182">https://github.com/NginxProxyManager/nginx-proxy-manager/blob/v2.16.0/backend/internal/token.js#L154-L182</a><br><a href="https://github.com/NginxProxyManager/nginx-proxy-manager/pull/5908">https://github.com/NginxProxyManager/nginx-proxy-manager/pull/5908</a><br><a href="https://www.vulncheck.com/advisories/nginx-proxy-manager-through-2.16.0-missing-brute-force-protection">https://www.vulncheck.com/advisories/nginx-proxy-manager-through-2.16.0-missing-brute-force-protection</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-2026-101280</a> | 7,3       | Trusted Domain Project<br>OpenDMARC                                               | Improper Authentication; Authentication Bypass by Spoofing                                 | up to 1.4.2.                                                                                            | <a href="https://vuldb.com/cve/CVE-2026-101280">https://vuldb.com/cve/CVE-2026-101280</a><br><a href="https://vuldb.com/submit/918282">https://vuldb.com/submit/918282</a><br><a href="https://vuldb.com/vuln/411037">https://vuldb.com/vuln/411037</a><br><a href="https://vuldb.com/vuln/411037/ctj">https://vuldb.com/vuln/411037/ctj</a><br><a href="https://xuvongzhe-vt.github.io/share/opendmarc-multi-record-downgrade.html">https://xuvongzhe-vt.github.io/share/opendmarc-multi-record-downgrade.html</a>                                                                             |              |             |                  |
| <a href="#">CVE-2026-102248</a> | 7,3       | Rebuild                                                                           | Improper Authentication                                                                    | up to 4.4.7                                                                                             | <a href="https://github.com/ASantsSec/CVE/issues/25">https://github.com/ASantsSec/CVE/issues/25</a><br><a href="https://vuldb.com/cve/CVE-2026-102248">https://vuldb.com/cve/CVE-2026-102248</a><br><a href="https://vuldb.com/submit/933708">https://vuldb.com/submit/933708</a><br><a href="https://vuldb.com/vuln/411150">https://vuldb.com/vuln/411150</a><br><a href="https://vuldb.com/vuln/411150/ctj">https://vuldb.com/vuln/411150/ctj</a>                                                                                                                                             |              |             |                  |
| <a href="#">CVE-2026-102293</a> | 7,3       | realjerrytang<br>tacomall                                                         | Incorrect Privilege Assignment; Improper Authorization                                     | 1.0.0                                                                                                   | <a href="https://github.com/fangtang7/CVE/blob/main/tacomall/create.md">https://github.com/fangtang7/CVE/blob/main/tacomall/create.md</a><br><a href="https://vuldb.com/cve/CVE-2026-102293">https://vuldb.com/cve/CVE-2026-102293</a><br><a href="https://vuldb.com/submit/941875">https://vuldb.com/submit/941875</a><br><a href="https://vuldb.com/vuln/411186">https://vuldb.com/vuln/411186</a><br><a href="https://vuldb.com/vuln/411186/ctj">https://vuldb.com/vuln/411186/ctj</a>                                                                                                       |              |             |                  |
| <a href="#">CVE-2026-86330</a>  | 7,2       | the set_host-name_internal<br>function of<br>NooBaa's cluster_internal_api        | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |                                                                                                         | <a href="https://access.redhat.com/security/cve/CVE-2026-86330">https://access.redhat.com/security/cve/CVE-2026-86330</a><br><a href="https://bugzilla.redhat.com/show_bug.cgi?id=2529295">https://bugzilla.redhat.com/show_bug.cgi?id=2529295</a>                                                                                                                                                                                                                                                                                                                                              |              |             |                  |
| <a href="#">CVE-2026-96326</a>  | 7,2       | The HT Contact Form – Drag & Drop Form Builder for WordPress plugin for WordPress | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')       | up to, and including, 2.10.2                                                                            | <a href="https://plugins.trac.wordpress.org/changeset/3714946/">https://plugins.trac.wordpress.org/changeset/3714946/</a><br><a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/782bcc9b-222e-4fee-a9c4-563e64dda1fd?source=cve">https://www.wordfence.com/threat-intel/vulnerabilities/id/782bcc9b-222e-4fee-a9c4-563e64dda1fd?source=cve</a>                                                                                                                                                                                                                                  |              |             |                  |
| <a href="#">CVE-2026-101044</a> | 7,1       | the pnpm npm package                                                              | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')             | >=12.0.0-alpha;<br><12.0.0-alpha.5                                                                      | <a href="https://github.com/pnpm/pnpm/security/advisories/GHSA-2rx9-3q3h-c2iv">https://github.com/pnpm/pnpm/security/advisories/GHSA-2rx9-3q3h-c2iv</a><br><a href="https://www.vulncheck.com/advisories/pacquet-before-12.0.0-alpha.5-path-traversal-via-lockfile-alias">https://www.vulncheck.com/advisories/pacquet-before-12.0.0-alpha.5-path-traversal-via-lockfile-alias</a>                                                                                                                                                                                                              |              |             |                  |
| <a href="#">CVE-2026-101059</a> | 7,1       | utcp-http                                                                         | Server-Side Request Forgery (SSRF)                                                         | before 1.1.4                                                                                            | <a href="https://github.com/universal-tool-calling-protocol/python-utcp/security/advisories/GHSA-8cp3-gxi6-px34">https://github.com/universal-tool-calling-protocol/python-utcp/security/advisories/GHSA-8cp3-gxi6-px34</a><br><a href="https://www.vulncheck.com/advisories/utcp-http-before-1.1.4-oauth2-tokenurl-trust-boundary-bypass">https://www.vulncheck.com/advisories/utcp-http-before-1.1.4-oauth2-tokenurl-trust-boundary-bypass</a>                                                                                                                                                | poc          | no          | partial          |
| <a href="#">CVE-2026-55096</a>  | 7,1       | fast-mcp-telegram                                                                 | Incomplete List of Disallowed Inputs; Server-Side Request Forgery (SSRF)                   | Prior to version 30.1                                                                                   | <a href="https://github.com/leshchenko1979/fast-mcp-telegram/commit/e6b3032cfc906e14f5b84f2c2b8ec378eb457e57">https://github.com/leshchenko1979/fast-mcp-telegram/commit/e6b3032cfc906e14f5b84f2c2b8ec378eb457e57</a><br><a href="https://github.com/leshchenko1979/fast-mcp-telegram/releases/tag/0.30.1">https://github.com/leshchenko1979/fast-mcp-telegram/releases/tag/0.30.1</a><br><a href="https://github.com/leshchenko1979/fast-mcp-telegram/security/advisories/GHSA-xr72-i7vj-vp7q">https://github.com/leshchenko1979/fast-mcp-telegram/security/advisories/GHSA-xr72-i7vj-vp7q</a> |              |             |                  |
| <a href="#">CVE-2026-87114</a>  | 7,1       | kube-compare                                                                      | Inclusion of Functionality from Untrusted Control Sphere                                   |                                                                                                         | <a href="https://access.redhat.com/security/cve/CVE-2026-87114">https://access.redhat.com/security/cve/CVE-2026-87114</a><br><a href="https://bugzilla.redhat.com/show_bug.cgi?id=2522945">https://bugzilla.redhat.com/show_bug.cgi?id=2522945</a>                                                                                                                                                                                                                                                                                                                                              |              |             |                  |
| <a href="#">CVE-2026-93538</a>  | 7,1       | SUSE Rancher Fleet                                                                | Authentication Bypass by Spoofing; Authorization Bypass Through User-Controlled Key        | 0; before 0.16.1, 0.15; before 0.15.6, 0.14; before 0.14.10, 0.13; before 0.13.15, 0.12; before 0.12.19 | <a href="https://github.com/rancher/fleet/security/advisories/GHSA-h9p5-fp5h-gpqr">https://github.com/rancher/fleet/security/advisories/GHSA-h9p5-fp5h-gpqr</a>                                                                                                                                                                                                                                                                                                                                                                                                                                 | none         | no          | partial          |
| <a href="#">CVE-2026-94286</a>  | 7,1       | libXtst's RECORD<br>reply parser in<br>libXtst                                    | Buffer Over-read                                                                           | before 1.2.6                                                                                            | <a href="https://gitlab.freedesktop.org/xorg/lib/libxtst/-/merge_requests/10/diffs?commit_id=16023c86070e6af9407330deea3938fcef75815b">https://gitlab.freedesktop.org/xorg/lib/libxtst/-/merge_requests/10/diffs?commit_id=16023c86070e6af9407330deea3938fcef75815b</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-2026-97023</a>  | 7,1       | Flatpak's handling of the export/bin directory during app deployment | UNIX Symbolic Link (Sym-link) Following                                                    |                                    | <a href="https://access.redhat.com/security/cve/CVE-2026-97023">https://access.redhat.com/security/cve/CVE-2026-97023</a><br><a href="https://github.com/flatpak/flatpak/security/advisories/GHSA-5p67-xh8x-rq54">https://github.com/flatpak/flatpak/security/advisories/GHSA-5p67-xh8x-rq54</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | none         | no          | partial          |
| <a href="#">CVE-2026-97024</a>  | 7,1       | Flatpak's handling of the files/etc directory during app deployment  | UNIX Symbolic Link (Sym-link) Following                                                    |                                    | <a href="https://access.redhat.com/security/cve/CVE-2026-97024">https://access.redhat.com/security/cve/CVE-2026-97024</a><br><a href="https://bugzilla.redhat.com/show_bug.cgi?id=2542625">https://bugzilla.redhat.com/show_bug.cgi?id=2542625</a><br><a href="https://github.com/flatpak/flatpak/security/advisories/GHSA-8xqg-v545-vqv1">https://github.com/flatpak/flatpak/security/advisories/GHSA-8xqg-v545-vqv1</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |              |             |                  |
| <a href="#">CVE-2026-100504</a> | 7,0       | Ghidra versions                                                      | Out-of-bounds Write                                                                        | through 12.1.4                     | <a href="https://github.com/NationalSecurityAgency/ghidra">https://github.com/NationalSecurityAgency/ghidra</a><br><a href="https://github.com/NationalSecurityAgency/ghidra/blob/8b6bbb857accdfa20dc5b2f5dea471178c2e9fbc/Ghidra/Features/Decompiler/src/decompile/cpp/multiprecision.cc#L29-L61">https://github.com/NationalSecurityAgency/ghidra/blob/8b6bbb857accdfa20dc5b2f5dea471178c2e9fbc/Ghidra/Features/Decompiler/src/decompile/cpp/multiprecision.cc#L29-L61</a><br><a href="https://github.com/NationalSecurityAgency/ghidra/blob/8b6bbb857accdfa20dc5b2f5dea471178c2e9fbc/Ghidra/Features/Decompiler/src/decompile/cpp/ruleaction.cc#L7848-L7878">https://github.com/NationalSecurityAgency/ghidra/blob/8b6bbb857accdfa20dc5b2f5dea471178c2e9fbc/Ghidra/Features/Decompiler/src/decompile/cpp/ruleaction.cc#L7848-L7878</a><br><a href="https://github.com/NationalSecurityAgency/ghidra/commit/6babe3c1cec7f5ec920dd16cdc86a02893e5b33c">https://github.com/NationalSecurityAgency/ghidra/commit/6babe3c1cec7f5ec920dd16cdc86a02893e5b33c</a><br><a href="https://www.vulncheck.com/advisories/ghidra-through-12.1.4-stack-based-buffer-overflow-via-leftshift128">https://www.vulncheck.com/advisories/ghidra-through-12.1.4-stack-based-buffer-overflow-via-leftshift128</a> | none         | no          | total            |
| <a href="#">CVE-2026-101032</a> | 7,0       | navi                                                                 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | through 2.24.0                     | <a href="https://github.com/denisidoro/navi">https://github.com/denisidoro/navi</a><br><a href="https://github.com/denisidoro/navi/blob/5515367dc8a2a561d2d82b8352f729b1da4120d3/src/commands/core/actor.rs#L159-L193">https://github.com/denisidoro/navi/blob/5515367dc8a2a561d2d82b8352f729b1da4120d3/src/commands/core/actor.rs#L159-L193</a><br><a href="https://github.com/denisidoro/navi/blob/5515367dc8a2a561d2d82b8352f729b1da4120d3/src/common/shell.rs#L39-L50">https://github.com/denisidoro/navi/blob/5515367dc8a2a561d2d82b8352f729b1da4120d3/src/common/shell.rs#L39-L50</a><br><a href="https://github.com/denisidoro/navi/issues/1037">https://github.com/denisidoro/navi/issues/1037</a><br><a href="https://www.vulncheck.com/advisories/navi-through-2.24.0-os-command-injection-via-cheatsheet-variables">https://www.vulncheck.com/advisories/navi-through-2.24.0-os-command-injection-via-cheatsheet-variables</a>                                                                                                                                                                                                                                                                                                                                                     | none         | no          | total            |
| <a href="#">CVE-2026-102010</a> | 7,0       | GCC                                                                  | Expired Pointer Dereference                                                                |                                    | <a href="https://access.redhat.com/security/cve/CVE-2026-102010">https://access.redhat.com/security/cve/CVE-2026-102010</a><br><a href="https://bugzilla.redhat.com/show_bug.cgi?id=2478395">https://bugzilla.redhat.com/show_bug.cgi?id=2478395</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.

| Σύντομη περιγραφή / Τίτλος                                                                 | Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες                                                                                                                                                                                                                                                                                                                                          | URL                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway   CISA</b> | <ul style="list-style-type: none"> <li>• <a href="#">CVE-2026-88771</a></li> <li>• <a href="#">CVE-2026-88772</a></li> <li>• <a href="#">CVE-2026-88773</a></li> <li>• <a href="#">CVE-2026-88774</a></li> <li>• <a href="#">CVE-2026-88775</a></li> <li>• <a href="#">CVE-2026-88776</a></li> <li>• <a href="#">CVE-2026-88777</a></li> <li>• <a href="#">CVE-2026-88778</a></li> </ul> | <a href="https://cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway">https://cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway</a> |
| <b>CISA Adds Two Known Exploited Vulnerabilities to Catalog   CISA</b>                     | <ul style="list-style-type: none"> <li>▪ <a href="#">CVE-2026-88771</a> Citrix NetScaler Improper Input Validation Vulnerability</li> <li>▪ <a href="#">CVE-2026-88772</a> Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability</li> </ul>                                                                                             | <a href="https://cisa.gov/news-events/alerts/2026/09/27/cisa-adds-two-known-exploited-vulnerabilities-catalog">https://cisa.gov/news-events/alerts/2026/09/27/cisa-adds-two-known-exploited-vulnerabilities-catalog</a>                                       |

## 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                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fake VPN Extensions Hijack Browser Traffic Through Hidden Proxy Servers</b>                       | <a href="https://cybersecuritynews.com/fake-vpn-extensions-hijack-browser-traffic">https://cybersecuritynews.com/fake-vpn-extensions-hijack-browser-traffic</a>                                                                           |
| <b>Dutch police confirm arrest in ShinyHunters hacking investigation</b>                             | <a href="https://bleepingcomputer.com/news/security/dutch-police-confirm-arrest-in-shinyhunters-hacking-investigation">https://bleepingcomputer.com/news/security/dutch-police-confirm-arrest-in-shinyhunters-hacking-investigation</a>   |
| <b>Over 16,000 Supabase databases expose PII, passwords, auth tokens</b>                             | <a href="https://bleepingcomputer.com/news/security/misconfigured-supabase-apps-expose-data-in-over-16-000-databases">https://bleepingcomputer.com/news/security/misconfigured-supabase-apps-expose-data-in-over-16-000-databases</a>     |
| <b>AI Agents Are Privileged Users; Who Is Auditing Their Access?</b>                                 | <a href="https://darkreading.com/vulnerabilities-threats/ai-agents-are-privileged-users-who-is-auditing-their-access">https://darkreading.com/vulnerabilities-threats/ai-agents-are-privileged-users-who-is-auditing-their-access</a>     |
| <b>Modulate Raises \$25 Million to Advance Deepfake Detection</b>                                    | <a href="https://securityweek.com/modulate-raises-25-million-to-advance-deepfake-detection">https://securityweek.com/modulate-raises-25-million-to-advance-deepfake-detection</a>                                                         |
| <b>Chrome Store Hosts 'Poper Blocker' Spyware Downloaded by Millions</b>                             | <a href="https://darkreading.com/application-security/chrome-store-poper-blocker-spyware-downloaded-millions">https://darkreading.com/application-security/chrome-store-poper-blocker-spyware-downloaded-millions</a>                     |
| <b>Florida AG Seeks Emergency Injunction to Restrict OpenAI and ChatGPT Over AI Safety Risks</b>     | <a href="https://cybersecuritynews.com/florida-ag-seeks-emergency-injunction-on-chatgpt">https://cybersecuritynews.com/florida-ag-seeks-emergency-injunction-on-chatgpt</a>                                                               |
| <b>JadePuffer agentic AI attacks target Azure, destroy cloud resources</b>                           | <a href="https://bleepingcomputer.com/news/security/jadepuffer-agentic-ai-attacks-target-azure-destroy-cloud-resources">https://bleepingcomputer.com/news/security/jadepuffer-agentic-ai-attacks-target-azure-destroy-cloud-resources</a> |
| <b>JadePuffer AI Actor Compromises Azure in Destructive Cloud Attack</b>                             | <a href="https://darkreading.com/cloud-security/jadepuffer-ai-actor-azure-tenant-destructive-cloud-attack">https://darkreading.com/cloud-security/jadepuffer-ai-actor-azure-tenant-destructive-cloud-attack</a>                           |
| <b>Call for Presentations Open for 2026 CISO Forum Virtual Summit</b>                                | <a href="https://securityweek.com/call-for-presentations-open-for-2026-ciso-forum-virtual-summit">https://securityweek.com/call-for-presentations-open-for-2026-ciso-forum-virtual-summit</a>                                             |
| <b>Bitget Restarts Bitcoin Withdrawals Following \$387.5m Wallet Breach</b>                          | <a href="https://infosecurity-magazine.com/news/bitget-restarts-withdrawals-387-5m">https://infosecurity-magazine.com/news/bitget-restarts-withdrawals-387-5m</a>                                                                         |
| <b>New File Notification Attack Lets Hackers Track User Activity Across Linux, Windows and macOS</b> | <a href="https://cybersecuritynews.com/new-file-notification-attack">https://cybersecuritynews.com/new-file-notification-attack</a>                                                                                                       |

|                                                                                         |                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hackers Built an AI-Powered Attack Machine and Accidentally Left the Control Panel Open | <a href="https://cybersecuritynews.com/ai-powered-attack-machine">https://cybersecuritynews.com/ai-powered-attack-machine</a>                                                                                                           |
| NVIDIA Launches Open Platform to Secure Autonomous AI Agents                            | <a href="https://infosecurity-magazine.com/news/nvidia-open-platform-secure">https://infosecurity-magazine.com/news/nvidia-open-platform-secure</a>                                                                                     |
| Deepfakes Are Becoming a Costly Reality for Businesses, Report Warns                    | <a href="https://infosecurity-magazine.com/news/deepfakes-costly-reality-for">https://infosecurity-magazine.com/news/deepfakes-costly-reality-for</a>                                                                                   |
| OpenAI Agent Swarm Bypassed Sandbox Limits and Left 80,000 Attack Payloads Behind       | <a href="https://cybersecuritynews.com/openai-agent-swarm-bypassed-sandbox">https://cybersecuritynews.com/openai-agent-swarm-bypassed-sandbox</a>                                                                                       |
| DC Health Agency Exposes 400,000 Beneficiary Records                                    | <a href="https://securityweek.com/dc-health-agency-exposes-400000-beneficiary-records">https://securityweek.com/dc-health-agency-exposes-400000-beneficiary-records</a>                                                                 |
| Google Warns of ShinyHunters' Fresh Oracle PeopleSoft Campaign                          | <a href="https://securityweek.com/google-warns-of-shinyhunters-fresh-oracle-peoplesoft-campaign">https://securityweek.com/google-warns-of-shinyhunters-fresh-oracle-peoplesoft-campaign</a>                                             |
| New Mexico Jury Finds Facebook Liable for Deceiving Users About Privacy Protections     | <a href="https://securityweek.com/new-mexico-jury-finds-facebook-liable-for-deceiving-users-about-privacy-protections">https://securityweek.com/new-mexico-jury-finds-facebook-liable-for-deceiving-users-about-privacy-protections</a> |
| Nvidia Unveils AI Agent Safety Platform With Hardware-Based Watchdog                    | <a href="https://securityweek.com/nvidia-unveils-ai-agent-safety-platform-with-hardware-based-watchdog">https://securityweek.com/nvidia-unveils-ai-agent-safety-platform-with-hardware-based-watchdog</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                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pentagon Data Breach - Hackers Reportedly Accessed 3 Million People's Sensitive Data | <a href="https://cybersecuritynews.com/pentagon-data-breach">https://cybersecuritynews.com/pentagon-data-breach</a>                                                                                                                     |
| Times Car confirms data breach affecting 6.6 million user accounts                   | <a href="https://bleepingcomputer.com/news/security/times-car-confirms-data-breach-affecting-66-million-user-accounts">https://bleepingcomputer.com/news/security/times-car-confirms-data-breach-affecting-66-million-user-accounts</a> |
| Prison Sentence for Former US Soldier Who Hacked AT&T and Verizon                    | <a href="https://securityweek.com/prison-sentence-for-former-us-soldier-who-hacked-att-and-verizon">https://securityweek.com/prison-sentence-for-former-us-soldier-who-hacked-att-and-verizon</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                                                                                                                                                                   |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical WatchGuard API Vulnerabilities Enables Command Execution Attacks      | <a href="https://cybersecuritynews.com/watchguard-api-vulnerabilities">https://cybersecuritynews.com/watchguard-api-vulnerabilities</a>                               |
| Critical Apple Zero-Day Vulnerability Actively Exploited in Attacks            | <a href="https://cybersecuritynews.com/apple-zero-day-vulnerability-exploited">https://cybersecuritynews.com/apple-zero-day-vulnerability-exploited</a>               |
| Official MCP Python SDK Flaw Can Let Malicious Servers Steal OAuth Credentials | <a href="https://thehackernews.com/2026/09/official-mcp-python-sdk-flaw-can-let.html">https://thehackernews.com/2026/09/official-mcp-python-sdk-flaw-can-let.html</a> |
| One Packet Can Crash OT Servers in Industrial Sectors                          | <a href="https://darkreading.com/ics-ot-security/one-packet-crash-servers-tdengine">https://darkreading.com/ics-ot-security/one-packet-crash-servers-tdengine</a>     |

|                                                                                                 |                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bitget Says Attacker Exploited Third-Party Security Product Flaw to Steal \$388M                | <a href="https://thehackernews.com/2026/09/bitget-says-attacker-exploited-third.html">https://thehackernews.com/2026/09/bitget-says-attacker-exploited-third.html</a>                                                                               |
| NCSC Urges UK organizations to Patch for Citrix NetScaler ADC and Gateway 0-Day Vulnerabilities | <a href="https://cybersecuritynews.com/citrix-netscaler-0-day-vulnerabilities">https://cybersecuritynews.com/citrix-netscaler-0-day-vulnerabilities</a>                                                                                             |
| CISA Warns of Microsoft SharePoint Code Injection Vulnerability Exploited in Attacks            | <a href="https://cybersecuritynews.com/microsoft-sharepoint-code-injection">https://cybersecuritynews.com/microsoft-sharepoint-code-injection</a>                                                                                                   |
| Kiteworks Urges Server Shutdown, Finds Advanced Forms Vulnerability                             | <a href="https://securityweek.com/kiteworks-urges-server-shutdown-finds-advanced-forms-vulnerability">https://securityweek.com/kiteworks-urges-server-shutdown-finds-advanced-forms-vulnerability</a>                                               |
| CISA Warns of Citrix NetScaler 0-Day RCE Vulnerabilities Exploited in Attacks                   | <a href="https://cybersecuritynews.com/citrix-netscaler-0-day-rce-vulnerabilities-exploited">https://cybersecuritynews.com/citrix-netscaler-0-day-rce-vulnerabilities-exploited</a>                                                                 |
| Citrix Confirms 2 NetScaler Zero-Days After Admins Pulled the Plug                              | <a href="https://securityweek.com/citrix-confirms-2-netscaler-zero-days-after-admins-pulled-the-plug">https://securityweek.com/citrix-confirms-2-netscaler-zero-days-after-admins-pulled-the-plug</a>                                               |
| CISA Says Attackers Are Exploiting Two Critical Citrix NetScaler Flaws Globally                 | <a href="https://thehackernews.com/2026/09/cisa-says-attackers-are-exploiting-two.html">https://thehackernews.com/2026/09/cisa-says-attackers-are-exploiting-two.html</a>                                                                           |
| Hackers Exploit GlobalProtect Flaw and Turn Stolen Data Into 2.4 Million Fraud Messages         | <a href="https://cybersecuritynews.com/hackers-exploit-globalprotect-flaw">https://cybersecuritynews.com/hackers-exploit-globalprotect-flaw</a>                                                                                                     |
| CISA orders feds to patch exploited Citrix flaws by Wednesday                                   | <a href="https://bleepingcomputer.com/news/security/cisa-orders-feds-to-patch-exploited-citrix-flaws-by-wednesday">https://bleepingcomputer.com/news/security/cisa-orders-feds-to-patch-exploited-citrix-flaws-by-wednesday</a>                     |
| Citrix Confirms NetScaler 0-Day RCE Vulnerabilities Actively Exploited in Attack                | <a href="https://cybersecuritynews.com/citrix-confirms-netscaler-0-day">https://cybersecuritynews.com/citrix-confirms-netscaler-0-day</a>                                                                                                           |
| Citrix confirms two NetScaler RCE zero-days exploited in attacks                                | <a href="https://bleepingcomputer.com/news/security/citrix-admins-warned-to-shut-down-netscalers-over-2-exploited-zero-days">https://bleepingcomputer.com/news/security/citrix-admins-warned-to-shut-down-netscalers-over-2-exploited-zero-days</a> |
| Microsoft SharePoint Flaw CVE-2026-65660 Now Exploited in Attacks                               | <a href="https://securityweek.com/microsoft-sharepoint-flaw-cve-2026-65660-now-exploited-in-attacks">https://securityweek.com/microsoft-sharepoint-flaw-cve-2026-65660-now-exploited-in-attacks</a>                                                 |
| ShinyHunters uses WAF bypass trick in Oracle PeopleSoft attacks                                 | <a href="https://bleepingcomputer.com/news/security/shinyhunters-uses-waf-bypass-trick-in-oracle-peoplesoft-attacks">https://bleepingcomputer.com/news/security/shinyhunters-uses-waf-bypass-trick-in-oracle-peoplesoft-attacks</a>                 |
| Attackers Bypass WAFs to Exploit Oracle PeopleSoft Flaw and Deploy Web Shells                   | <a href="https://thehackernews.com/2026/09/attackers-bypass-wafs-to-exploit-oracle.html">https://thehackernews.com/2026/09/attackers-bypass-wafs-to-exploit-oracle.html</a>                                                                         |
| Elementor CSRF Flaw Lets Attackers Take Over Sites After Admin Clicks Crafted Link              | <a href="https://thehackernews.com/2026/09/elementor-csrf-flaw-lets-attackers-take.html">https://thehackernews.com/2026/09/elementor-csrf-flaw-lets-attackers-take.html</a>                                                                         |
| SharePoint RCE and MikroTik RouterOS Flaws Actively Exploited in the Wild                       | <a href="https://thehackernews.com/2026/09/sharepoint-rce-and-mikrotik-routeros.html">https://thehackernews.com/2026/09/sharepoint-rce-and-mikrotik-routeros.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                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apple patches CoreGraphics zero-day flaw exploited in attacks                   | <a href="https://bleepingcomputer.com/news/security/apple-patches-coregraphics-zero-day-flaw-exploited-in-attacks">https://bleepingcomputer.com/news/security/apple-patches-coregraphics-zero-day-flaw-exploited-in-attacks</a> |
| Apple Patches Meta-Reported Zero-Day Linked to 'Extremely Sophisticated Attack' | <a href="https://securityweek.com/apple-patches-meta-reported-zero-day-linked-to-extremely-sophisticated-attack">https://securityweek.com/apple-patches-meta-reported-zero-day-linked-to-extremely-sophisticated-attack</a>     |
| Apple Patches CoreGraphics Flaw Possibly Exploited in Targeted Attacks          | <a href="https://thehackernews.com/2026/09/apple-patches-coregraphics-flaw.html">https://thehackernews.com/2026/09/apple-patches-coregraphics-flaw.html</a>                                                                     |

|                                                                                        |                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PHP Fixed a Bug That Could Send Your Login Credentials to the Wrong Server             | <a href="https://cybersecuritynews.com/php-fixed-a-bug">https://cybersecuritynews.com/php-fixed-a-bug</a>                                                                                                                                     |
| Citrix Patches Critical Zero Days Under Active Exploitation                            | <a href="https://infosecurity-magazine.com/news/citrix-patches-critical-zero-days">https://infosecurity-magazine.com/news/citrix-patches-critical-zero-days</a>                                                                               |
| Wireshark 4.6.9 Fixes 19 Vulnerabilities Including Code Execution Via Malicious Packet | <a href="https://cybersecuritynews.com/wireshark-4-6-9-fixes-19-vulnerabilities">https://cybersecuritynews.com/wireshark-4-6-9-fixes-19-vulnerabilities</a>                                                                                   |
| Cloudflare fixes Containers cross-tenant flaw exposing customer data                   | <a href="https://bleepingcomputer.com/news/security/cloudflare-fixes-containers-cross-tenant-flaw-exposing-customer-data">https://bleepingcomputer.com/news/security/cloudflare-fixes-containers-cross-tenant-flaw-exposing-customer-data</a> |
| Warning: Two Unpatched Citrix NetScaler RCE Zero-Days Under Active Exploitation        | <a href="https://thehackernews.com/2026/09/warning-two-unpatched-citrix-netscaler.html">https://thehackernews.com/2026/09/warning-two-unpatched-citrix-netscaler.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                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BotHelper RAT Uses Encrypted Payloads and Live Screen Surveillance to Spy on Windows Users     | <a href="https://cybersecuritynews.com/bothelper-rat">https://cybersecuritynews.com/bothelper-rat</a>                                                                                                                                   |
| Japan's Keio confirms ransomware attack disrupted business systems                             | <a href="https://bleepingcomputer.com/news/security/japans-keio-confirms-ransomware-attack-disrupted-business-systems">https://bleepingcomputer.com/news/security/japans-keio-confirms-ransomware-attack-disrupted-business-systems</a> |
| Microsoft Finds New Malware Used by Hackers to Maintain Secret Access Inside Target Networks   | <a href="https://cybersecuritynews.com/needymantis-malware-secret-network-access">https://cybersecuritynews.com/needymantis-malware-secret-network-access</a>                                                                           |
| ⚡ Weekly Recap: \$387M Crypto Hack, Citrix Exploits, AI Agents Go Off-Script, and More Threats | <a href="https://thehackernews.com/2026/09/weekly-recap-387m-crypto-hack-citrix.html">https://thehackernews.com/2026/09/weekly-recap-387m-crypto-hack-citrix.html</a>                                                                   |
| Lunex Stealer Abuses AMD Driver to Disable Security Monitoring and Steal Browser Credentials   | <a href="https://thehackernews.com/2026/09/lunex-stealer-abuses-amd-driver-to.html">https://thehackernews.com/2026/09/lunex-stealer-abuses-amd-driver-to.html</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 |
|-------------------------------------------------------------|-----|
| Δεν εντοπίστηκαν άρθρα για το καθορισμένο χρονικό διάστημα. |     |

## 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 26/09/2026–29/09/2026, 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>                                                                                                                                                                                                                 |