

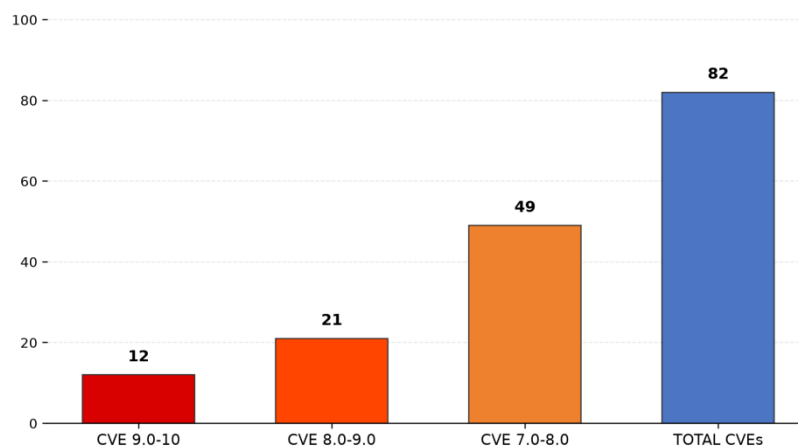


Newsletter on system vulnerabilities and
cybersecurity news.

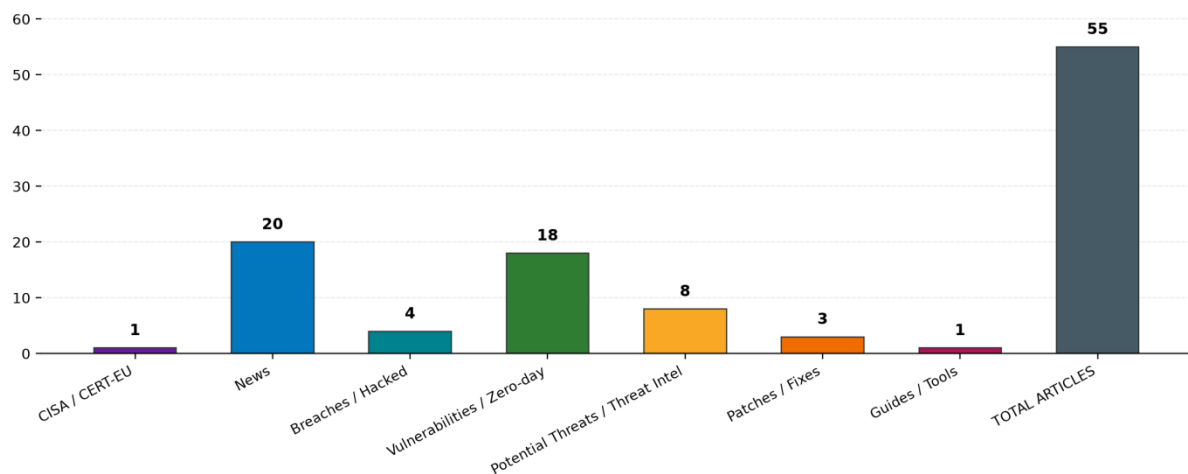
National Cyber Security Authority (NCSA)

Date: 03/10/2026 - 06/10/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories.....	20
News.....	20
Breaches / Compromised / Hacked.....	21
Vulnerabilities / Flaws / Zero-day.....	22
Patches / Updates / Fixes	23
Potential threats / Threat intelligence	23
Guides / Tools.....	24
References.....	25
Annex – Websites with vendor specific vulnerabilities	26

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
CVE-2026-105134	10,0	Ahsay AhsayCBS	Improper Neutralization of Special Elements used in a Command ('Command Injection'); Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	up to 10.3.2.; version 10.3.4	https://vuldb.com/cve/CVE-2026-105134 https://vuldb.com/submit/942743 https://vuldb.com/vuln/413351 https://vuldb.com/vuln/413351/cti https://www.ahsay.com/en/support/help-centre/release-notes/cbs/v10.3.4	none	yes	total
CVE-2026-105135	10,0	InternLM MindSearch	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Control of Generation of Code ('Code Injection')	0.1.0	https://gist.github.com/DReazer/7ad46df9da73d0cf414276e4195b2183 https://vuldb.com/cve/CVE-2026-105135 https://vuldb.com/submit/943315 https://vuldb.com/vuln/413352 https://vuldb.com/vuln/413352/cti			
CVE-2026-105284	10,0	Totolink A3002MU	Incorrect Privilege Assignment; Improper Authorization	1.0.0-B20230403.1455	https://gist.github.com/H3rmesk1t/ac6e91a8fba51002be085755c8bf7d43 https://vuldb.com/cve/CVE-2026-105284 https://vuldb.com/submit/977217 https://vuldb.com/vuln/413465 https://vuldb.com/vuln/413465/cti https://www.totolink.net/	poc	yes	total
CVE-2026-105484	10,0	TOTOLINK X6000R	Improper Neutralization of Special Elements used in a Command ('Command Injection'); Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	9.4.0cu.652_B20230116	https://vuldb.com/cve/CVE-2026-105484 https://vuldb.com/submit/984434 https://vuldb.com/vuln/413619 https://vuldb.com/vuln/413619/cti https://www.totolink.net/			
CVE-2026-105080	9,9	In ConvertX	Inclusion of Functionality from Untrusted Control Sphere	before 0.19.0	https://github.com/C4illin/ConvertX/commit/0ca17dad7fa65e2e34823b59b95dd0bb1066b66 https://github.com/C4illin/ConvertX/releases/tag/v0.19.0 https://github.com/C4illin/ConvertX/security/advisories/GHSA-m4hh-ramf-c8hw			
CVE-2026-105697	9,9	Langflow	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 1.10.3)	https://github.com/langflow-ai/langflow/commit/eba285edf1dd4a33bf23a9cb8113c991fcd3d1d https://github.com/langflow-ai/langflow/commit/efbc4a16e639409d938a4883463d27ef0bc637a0 https://github.com/langflow-ai/langflow/pull/12290 https://github.com/langflow-ai/langflow/pull/14036 https://github.com/langflow-ai/langflow/releases/tag/v1.10.3 https://github.com/langflow-ai/langflow/security/advisories/GHSA-w794-ri3p-xv45			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-105778	9,9	Tenda AC5	Improper Restriction of Operations within the Bounds of a Memory Buffer; Stack-based Buffer Overflow	02.03.01.111_multi	https://github.com/raisecnul/Tenda-AC5v3-BOF/blob/main/blog.md https://vuldb.com/cve/CVE-2026-105778 https://vuldb.com/submit/992587 https://vuldb.com/vuln/413811 https://vuldb.com/vuln/413811/ctj https://www.tenda.com.cn/			
CVE-2026-88395	9,8	GouGuOA	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://github.com/fang-tang7/CVE/blob/main/GouGuOA/sql.md	poc	yes	total
CVE-2026-94293	9,8	Software AAS Edge Client all versions	Missing Authentication for Critical Function	0.0.0	https://www.certvde.com/en/advisories/VDE-2026-108/			
CVE-2026-97283	9,8	Liquid Web / StellarWP Advanced Post Manager advanced-post-manager	Deserialization of Untrusted Data	through 4.5.5.	https://patchstack.com/database/wordpress/plugin/advanced-post-manager/vulnerability/wordpress-advanced-post-manager-plugin-4-5-5-php-object-injection-vulnerability?_s_id=cve	none	yes	total
CVE-2026-87115	9,1	The VikAppointments Services Booking Calendar plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 1.2.21.	https://plugins.trac.wordpress.org/browser/vikappointments/tags/1.2.19/site/controllers/confirmapp.php#L88 https://plugins.trac.wordpress.org/browser/vikappointments/tags/1.2.19/site/helpers/libraries/customfields/types/file.php#L131 https://plugins.trac.wordpress.org/browser/vikappointments/tags/1.2.19/site/helpers/libraries/customfields/types/file.php#L53 https://plugins.trac.wordpress.org/browser/vikappointments/tags/1.2.19/vikappointments.php#L237 https://plugins.trac.wordpress.org/browser/vikappointments/tags/1.2.21/site/controllers/confirmapp.php#L88 https://plugins.trac.wordpress.org/browser/vikappointments/tags/1.2.21/site/helpers/libraries/customfields/types/file.php#L131	none	yes	partial
CVE-2026-92084	9,1	The The Beaver Builder Page Builder – Drag and Drop Website Builder plugin for WordPress	Improper Control of Generation of Code ('Code Injection')	up to, and including, 2.11.0.5.	https://plugins.trac.wordpress.org/browser/beaver-builder-lite-version/tags/2.11.0.5/classes/class-fl-builder-module.php#L143 https://plugins.trac.wordpress.org/browser/beaver-builder-lite-version/tags/2.11.0.5/classes/class-fl-builder.php#L2139 https://plugins.trac.wordpress.org/browser/beaver-builder-lite-version/tags/2.11.0.5/classes/class-fl-builder.php#L2264 https://plugins.trac.wordpress.org/browser/beaver-builder-lite-version/tags/2.11.0.5/modules/sidebar/includes/frontend.php#L4 https://plugins.trac.wordpress.org/browser/beaver-builder-lite-version/tags/2.11.0.5/modules/sidebar/sidebar.php#L11 https://plugins.trac.wordpress.org/changeset/3713226/beaver-builder-lite-version/trunk/modules/sidebar/sidebar.php	none	yes	total
CVE-2026-100511	8,8	Vektor Inc	Deserialization of Untrusted Data	through 1.3.1.	https://patchstack.com/database/wordpress/plugin/vk-google-job-posting-manager/vulnerability/wordpress-vk-google-job-posting-manager-plugin-1-3-1-php-object-injection-vulnerability?_s_id=cve			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-101919	8,8	the HyperShift operator	Improper Input Validation		https://access.redhat.com/security/cve/CVE-2026-101919 https://bugzilla.redhat.com/show_bug.cgi?id=2542541			
CVE-2026-105123	8,8	W (vincent-peugnet/wcms)	Unrestricted Upload of File with Dangerous Type	through 3.18.0	https://github.com/vincent-peugnet/wcms https://github.com/vincent-peugnet/wcms/blob/cda5bcd95dbdb1e804fdfe0e5fd2e2b2f8a90e2/app/class/Controllerapimedia.php#L24-L44 https://github.com/vincent-peugnet/wcms/blob/cda5bcd95dbdb1e804fdfe0e5fd2e2b2f8a90e2/app/class/Media.php#L98 https://github.com/vincent-peugnet/wcms/issues/662 https://www.vulncheck.com/advisories/w-wcms-through-3.18.0-rce-and-arbitrary-file-write-via-media-upload-api	none	no	total
CVE-2026-105642	8,8	Ghost	Improper Control of Generation of Code ('Code Injection')	>= 6.56.0, < 6.67.0	https://github.com/TryGhost/Ghost/security/advisories/GHSA-788w-68h3-cvxp	none	no	total
CVE-2026-105701	8,8	The ACPT (Premium) plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 2.0.66	https://acpt.io/changelog/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9cd544ed-493e-4d4a-9eb8-ea83c47f3857?source=cve			
CVE-2026-18443	8,8	The Smart Manager – Advanced WooCommerce Bulk Edit & Inventory Management plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 8.97.0	https://plugins.trac.wordpress.org/browser/smart-manager-for-wp-e-commerce/tags/8.92.0/common-core/classes/class-sa-manager-controller.php#L143 https://plugins.trac.wordpress.org/browser/smart-manager-for-wp-e-commerce/tags/8.92.0/pro/classes/class-smart-manager-pro-access-privilege.php#L38 https://plugins.trac.wordpress.org/browser/smart-manager-for-wp-e-commerce/tags/8.92.0/pro/classes/class-smart-manager-pro-access-privilege.php#L472 https://plugins.trac.wordpress.org/browser/smart-manager-for-wp-e-commerce/tags/8.92.0/pro/classes/class-smart-manager-pro-access-privilege.php#L99 https://plugins.trac.wordpress.org/browser/smart-manager-for-wp-e-commerce/tags/8.93.0/common-core/classes/class-sa-manager-controller.php#L143 https://plugins.trac.wordpress.org/browser/smart-manager-for-wp-e-commerce/tags/8.93.0/pro/classes/class-smart-manager-pro-access-privilege.php#L38	none	no	total
CVE-2026-20586	8,8	vdec	Out-of-bounds Write	MT2718; MT6768; MT6769; MT6789; MT6833; MT6855; MT6877; MT8186; MT8188; MT8189; MT8195; MT8196; MT8367; MT8391; MT8395; MT8668; MT8676; MT8678; MT8696; MT8781; MT8788E; MT8792; MT8793; MT8799; MT8910	https://www.mediatek.com/product-security-bulletin/October-2026	none	no	total
CVE-2026-45524	8,8	Android	Missing Authorization	17	https://source.android.com/docs/security/bulletin/2026/2026-10-01	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
CVE-2026-55280	8,8	In multiple locations, there	Use of Uninitialized Variable	17; 16-qpr2; 16	https://source.android.com/docs/security/bulletin/2026/2026-10-01	none	no	total
CVE-2026-88783	8,8	The Kubio AI Page Builder WordPress plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 2.9.3	https://wpscan.com/vulnerability/94d11df1-dae7-479f-bc93-3db6b0925d99/	none	no	total
CVE-2026-92536	8,8	Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress	Improper Control of Generation of Code ('Code Injection')	up to, and including, 4.17.4	https://plugins.trac.wordpress.org/browser/wp-user-avatar/tags/4.17.4/src/Classes/EditUserProfile.php#L342 https://plugins.trac.wordpress.org/browser/wp-user-avatar/tags/4.17.4/src/Classes/RegistrationAuth.php#L131 https://plugins.trac.wordpress.org/browser/wp-user-avatar/tags/4.17.4/src/Functions/GlobalFunctions.php#L1715 https://plugins.trac.wordpress.org/browser/wp-user-avatar/tags/4.17.4/src/ShortcodeParser/Builder/GlobalShortcodes.php#L165 https://plugins.trac.wordpress.org/browser/wp-user-avatar/tags/4.17.4/src/ShortcodeParser/FrontendProfileTag.php#L140 https://plugins.trac.wordpress.org/browser/wp-user-avatar/tags/4.17.4/src/ShortcodeParser/MemberDirectoryTag.php#L237	none	no	total
CVE-2026-92931	8,8	the Progress @progress/sitefinity-nextjs-sdk npm package	Server-Side Request Forgery (SSRF)	versions 15.1.8326 through 15.4.8637	https://community.progress.com/s/article/Sitefinity-Critical-Security-Advisory-for-Addressing-Security-Vulnerabilities-in-Next-is-September-2026	none	no	total
CVE-2026-93549	8,8	The CoCart WordPress plugin	Cross-Site Request Forgery (CSRF)	before 4.9.7	https://wpscan.com/vulnerability/77f413f6-8753-4c83-8623-00ad7a1dcaff/	none	no	total
CVE-2026-96451	8,8	Ultimate Member Ultimate Member ultimate-member	Authorization Bypass Through User-Controlled Key	through 2.13.1.	https://patchstack.com/database/wordpress/plugin/ultimate-member/vulnerability/wordpress-ultimate-member-plugin-2-13-1-privilege-escalation-vulnerability? s_id=cve	none	no	total
CVE-2026-97257	8,8	PressTigers Simple Event Planner simple-event-planner	Deserialization of Untrusted Data	through 1.5.7.	https://patchstack.com/database/wordpress/plugin/simple-event-planner/vulnerability/wordpress-simple-event-planner-plugin-1-5-7-php-object-injection-vulnerability? s_id=cve			
CVE-2026-97644	8,8	The Groundhogg — CRM, Newsletters, and Marketing Automation plugin for WordPress	Improper Privilege Management	up to, and including, 4.9	https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.8.3/api/v3/contacts-api.php#L373 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.8.3/api/v4/emails-api.php#L571 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.8.3/db/contacts.php#L205 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.8.3/includes/main-roles.php#L532 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.8.3/includes/replacements.php#L2280 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.8.3/includes/rewrites.php#L460	none	no	total
CVE-2026-105086	8,7	WWBN AVideo	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12.4 through 29.2.0	https://github.com/WWBN/AVideo/commit/c4b6ca95a0ae3efa09919a98879870086cf150e https://github.com/WWBN/AVideo/security/advisories/GHSA-q62w-927x-vhnh https://www.vulncheck.com/advisories/wwbn-avideo-12.4-through-29.2.0-stored-xss-via-double-encoded-video-title	poc	no	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-89236	8,6	The SaveTo Wish-list Lite WordPress plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 1.1.5	https://wpscan.com/vulnerability/7b92ed60-7bcb-4dcf-8c57-0afcaa6809b7/	none	yes	partial
CVE-2026-91078	8,2	The TillKit WordPress plugin	Improper Authentication	before 1.0.5	https://wpscan.com/vulnerability/7ab037d6-c670-4eaf-be0d-11cc9e20b18e/	none	yes	partial
CVE-2026-101923	8,1	The Photo Reviews for WooCommerce plugin for WordPress	Missing Authorization	up to, and including, 1.2.30.	https://plugins.trac.wordpress.org/browser/woo-photo-reviews/trunk/admin/admin.php#L2390 https://plugins.trac.wordpress.org/browser/woo-photo-reviews/trunk/admin/admin.php#L31 https://plugins.trac.wordpress.org/browser/woo-photo-reviews/trunk/frontend/frontend.php#L1232 https://plugins.trac.wordpress.org/browser/woo-photo-reviews/trunk/frontend/frontend.php#L1268 https://plugins.trac.wordpress.org/changeset?reponame=&old=3718551%40woo-photo-reviews&new=3718551%40woo-photo-reviews https://www.wordfence.com/threat-intel/vulnerabilities/id/bdc330ea-e490-43a5-93eb-a434a0e02868?source=cve	none	no	partial
CVE-2026-94505	8,1	The Nelio Content – Editorial Calendar & Social Media Auto-Posting plugin for WordPress	Missing Authorization	up to, and including, 4.5.0	https://plugins.trac.wordpress.org/browser/nelio-content/tags/4.5.0/includes/post-types/reusable-messages/class-nelio-content-reusable-message-rest-controller.php#L169 https://plugins.trac.wordpress.org/browser/nelio-content/tags/4.5.0/includes/post-types/reusable-messages/class-nelio-content-reusable-message-rest-controller.php#L68 https://plugins.trac.wordpress.org/browser/nelio-content/tags/4.5.0/includes/utils/functions/helpers.php#L80 https://plugins.trac.wordpress.org/changeset/3724505/nelio-content/tags/4.5.1 https://www.wordfence.com/threat-intel/vulnerabilities/id/828050ce-4775-4256-8dcf-2c9b96d5ec4e?source=cve	none	no	partial
CVE-2026-77805	7,9	In Progress® Telerik® Fiddler® Classic for Windows	Improper Verification of Cryptographic Signature	versions prior to v6.0.20262.10021	https://docs.telerik.com/fiddler/knowledge-base/kb-security-weak-executable-signature-verification-cve-2026-77805	none	no	total
CVE-2026-105220	7,8	Twine	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	through 2.12.0	https://github.com/klembot/twinejs https://github.com/klembot/twinejs/blob/2.12.0/src/election/main-process/scratch-file.ts#L57-L63 https://github.com/klembot/twinejs/blob/2.12.0/src/util/import.ts#L134-L136 https://github.com/klembot/twinejs/commit/3a9af28cabe9684730beb8b578132cad9bb5bc60 https://github.com/klembot/twinejs/commit/8e8a2bef5b1e20c58b99d22a2a4d8d867fb421cb https://github.com/klembot/twinejs/issues/1706	poc	no	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-12171	7,8	auto-changelog	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); Improper Neutralization of Argument Delimiters in a Command ('Argument Injection'); Improper Control of Generation of Code ('Code Injection'); Inclusion of Functionality from Untrusted Control Sphere; Server-Side Request Forgery (SSRF)	before 2.6.1	https://github.com/cookpete/auto-changelog/commit/1d02a48a0a57c69a3cd268aca375d64d50877c1a https://github.com/cookpete/auto-changelog/security/advisories/GHSA-xpvr-2hvx-m8q4	poc	no	total
CVE-2026-19185	7,8	drivers/i3c/i3c_handlers	Untrusted Pointer Dereference	3.2.0 prior to 4.5.0	https://github.com/zephyrproject-rtos/zephyr/commit/35562f22f40c6d2f31969a31f0a4902e5b067f27 https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-pcrr-29i7-8w57	none	no	partial

CVE-2026-25267	7,8	Snapdragon	Missing Authorization	315 5G IoT Modem; 5G Fixed Wireless Access Platform; 9205 LTE Modem; 9205S Modem; AQT1000; AR8031; AR8035; Cologne; CSRA6620; CSRA6640; CSRB31024; C-V2X 9150; FastConnect 6200; FastConnect 6700; FastConnect 6800; FastConnect 6900; FastConnect 7800; FSM100 Platform; G1 Gen 1; G3x Gen 2; IQ6 Series Platform; IQ8 Series Platform; IQ9 Series Platform; IQX5121; MBM415; Monaco_IOT; Networking Pro 1210 Platform; Networking Pro 1610 Platform; Networking Pro 610 Platform; Networking Pro 810 Platform; Q-4390; QCA0000; QCA4004; QCA6174A; QCA6391; QCA6420; QCA6421; QCA6426; QCA6430; QCA6431; QCA6436; QCA6564; QCA6564A; QCA6564AU; QCA6574; QCA6574A; QCA6574AU; QCA6595; QCA6595AU; QCA6688AQ; QCA6696; QCA6698AQ; QCA6698AU; QCA6797AQ; QCA8337; QCA9377; QCA9984; QCC2070; QCC6705; QCC710; QCC711; QCM2290; QCM4290; QCM4325; QCM5430; QCM6125; QCM6490; QCM8550; QCN7606; QCN9011; QCN9012; QCS2290; QCS410; QCS4290; QCS8155; QCS8550; QRB5165N; QSM8250; QSM8350; Qualcomm Dragonwing IQ-X; Qualcomm Dragonwing QCM4490; Qualcomm Dragonwing QRB5165;	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2026-bulletin.html			
--------------------------------	-----	------------	-----------------------	---	---	--	--	--

			Qualcomm QTS110 Tracker; Qualcomm Video Collaboration VC1 Platform; Qualcomm Video Collaboration VC3 Platform; Qualcomm Video Collaboration VC5 Platform; Robotics RB2 Platform; Robotics RB5 Platform; SA2150P; SA4150P; SA4155P; SA6145P; SA6150P; SA6155; SA6155P; SA8145P; SA8150P; SA8155; SA8155P; SA8195P; SC8180X+SDX55; SC8380XP; SD 675; SD 8 Gen1 5G; SD460; SD662; SD730; SD855; SD865 5G; SD888; SDA640; SDM640; SM4125; SM6225P; SM6250; SM6250P; SM6370; SM7315; SM7325P; SM8550P; Smart Audio 400 Platform; Snapdragon 4 Gen 1 Mobile Platform; Snapdragon 4 Gen 2 Mobile Platform; Snapdragon 460 Mobile Platform; Snapdragon 480 5G Mobile Platform; Snapdragon 480+ 5G Mobile Platform; Snapdragon 662 Mobile Platform; Snapdragon 665 Mobile Platform; Snapdragon 675 Mobile Platform; Snapdragon 678 Mobile Platform; Snapdragon 680 4G Mobile Platform; Snapdragon 685 4G Mobile Platform; Snapdragon 695 5G Mobile Platform; Snapdragon 720G Mobile Platform; Snapdragon 730 Mobile Platform; Snapdragon 730G Mobile Platform; Snapdragon 732G Mobile Platform; Snapdragon 778G 5G Mobile Platform; Snapdragon 778G+ 5G Mobile Platform; Snapdragon 780G 5G Mobile Platform;				
--	--	--	--	--	--	--	--

				Snapdragon 782G Mobile Platform; Snapdragon 7c Compute Platform; Snapdragon 7c Gen 2 Compute Platform "Rennell Pro"; Snapdragon 7c+ Gen 3 Compute; Snapdragon 8 Gen 1 Mobile Platform; Snapdragon 8 Gen 2 Mobile Platform; Snapdragon 8+ Gen 1 Mobile Platform; Snapdragon 8+ Gen 2 Mobile Platform; Snapdragon 855 Mobile Platform; Snapdragon 855+/860 Mobile Platform; Snapdragon 865 5G Mobile Platform; Snapdragon 865+ 5G Mobile Platform; Snapdragon 870 5G Mobile Platform; Snapdragon 888 5G Mobile Platform; Snapdragon 888+ 5G Mobile Platform; Snapdragon 8c Compute Platform "Poipu Lite"; Snapdragon 8c Compute Platform (SC8180XP-AD) "Poipu Lite"; Snapdragon 8cx Compute Platform; Snapdragon 8cx Compute Platform "Poipu Pro"; Snapdragon 8cx Gen 2 5G Compute Platform; Snapdragon 8cx Gen 2 5G Compute Platform "Poipu Pro"; Snapdragon Auto 5G Modem-RF; Snapdragon C Platform; Snapdragon Wear 1300 Platform; Snapdragon X24 LTE Modem; Snapdragon X50 5G Modem-RF System; Snapdragon X53 5G Modem-RF System; Snapdragon X55 5G Modem-RF System; Snapdragon XR2 5G Platform; Snapdragon XR2+ Gen 1 Platform; Snapdragon Auto 4G Modem; SXR2130; TalynPlus; Vision Intelli-				
--	--	--	--	---	--	--	--	--

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
				gence 300 Platform; Vision Intelligence 400 Platform; WCD9306; WCD9335; WCD9340; WCD9341; WCD9360; WCD9370; WCD9371; WCD9375; WCD9380; WCD9385; WCD9390; WCD9395; WCN3910; WCN3950; WCN3980; WCN3988; WCN3990; WCN3999; WCN6740; WSA8810; WSA8815; WSA8830; WSA8832; WSA8835; WSA8840; WSA8845; WSA8845H				
CVE-2026-55270	7,8	dialInternal	Unintended Proxy or Intermediary ('Confused Deputy')	17; 16-qpr2; 16; 15; 14	https://source.android.com/docs/security/bulletin/2026/2026-10-01	none	no	total
CVE-2026-58859	7,8		Uncaught Exception	17	https://source.android.com/docs/security/bulletin/2026/2026-10-01	none	no	total
CVE-2026-104408	7,6	Groundhogg	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	through 4.8.3.	https://patchstack.com/database/wordpress/plugin/groundhogg/vulnerability/wordpress-groundhogg-plugin-4-8-3-sql-injection-vulnerability? s_id=cve	none	no	partial
CVE-2026-97303	7,6	Apps Mav Scratch & Win – Giveaways and Contests scratch-win-giveaways-for-website-facebook	Missing Authorization	through 3.0.2.	https://patchstack.com/database/wordpress/plugin/scratch-win-giveaways-for-website-facebook/vulnerability/wordpress-scratch-win-giveaways-and-contests-plugin-3-0-2-broken-access-control-vulnerability? s_id=cve			
CVE-2026-101159	7,5	The WP Ultimate Review WordPress plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 2.4.4	https://wpscan.com/vulnerability/1eefa81e-6134-498b-9615-b9a42cd99749/	none	no	total
CVE-2026-103334	7,5	Etoile Web Design Incorporated Five Star Restaurant Reservations restaurant-reservations	Insertion of Sensitive Information Into Sent Data	through 2.7.24.	https://patchstack.com/database/wordpress/plugin/restaurant-reservations/vulnerability/wordpress-five-star-restaurant-reservations-plugin-2-7-24-sensitive-data-exposure-vulnerability? s_id=cve	none	yes	partial
CVE-2026-103514	7,5	The WP	Improper Authentication	before 4.1.0	https://wpscan.com/vulnerability/e05aa5a3-cd04-428a-b6bb-0538ca1f6b4a/	none	no	total
CVE-2026-103913	7,5	The GeoDirectory plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 2.8.186.	https://plugins.trac.wordpress.org/browser/geodirectory/tags/2.8.185/includes/class-geodir-ajax.php#L1464 https://plugins.trac.wordpress.org/browser/geodirectory/tags/2.8.185/includes/class-geodir-post-data.php#L660 https://plugins.trac.wordpress.org/browser/geodirectory/tags/2.8.185/includes/general-functions.php#L1312 https://plugins.trac.wordpress.org/browser/geodirectory/tags/2.8.185/includes/general-functions.php#L1394 https://plugins.trac.wordpress.org/browser/geodirectory/tags/2.8.185/includes/widgets/class-geodir-widget-listings.php#L862 https://plugins.trac.wordpress.org/changeset?reponame=&old=3723536%40geodirectory&new=3723536%40geodirectory	none	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-104891	7,5	mppx-condition-gate	Authentication Bypass by Spoofing; Incorrect Authorization	< b1d9935a57ba6d32da49eead1bfb459ad0cd55ab; < 3.0.0; < 1.0.4	https://github.com/insumerapi/mppx-condition-gate/commit/b1d9935a57ba6d32da49eead1bfb459ad0cd55ab https://github.com/insumerapi/mppx-condition-gate/commit/ec43a2fcd443a0fa102b6d4203abed2b785bd954 https://github.com/insumerapi/mppx-condition-gate/security/advisories/GHSA-q6g-3qfh-r9f8	none	yes	partial
CVE-2026-105072	7,5	FluentBooking Pro	Missing Authorization	< 2.5.0	https://patchstack.com/database/wordpress/plugin/fluent-booking-pro/vulnerability/wordpress-fluentbooking-pro-plugin-2-5-0-broken-access-control-vulnerability?_s_id=cve			
CVE-2026-105219	7,5	mammoth.js	Inefficient Regular Expression Complexity	before 1.12.3	https://github.com/mwilliamson/mammoth.js https://github.com/mwilliamson/mammoth.js/blob/1.12.2/lib/styles/parser/tokeniser.js#L6-L30 https://github.com/mwilliamson/mammoth.js/commit/dc49225425c2c07de0a6dc3529f2386c82a032b4 https://github.com/mwilliamson/mammoth.js/issues/487 https://www.vulncheck.com/advisories/mammoth-is-1.3.0-before-1.12.3-redos-via-style-map-tokeniser	none	yes	partial
CVE-2026-105295	7,5	GitAhead	Download of Code Without Integrity Check	2.5.0 through 2.7.1	https://github.com/gitahed/gitahed https://github.com/gitahed/gitahed/blob/v2.7.1/src/appl/Application.cpp#L284-L309 https://github.com/gitahed/gitahed/blob/v2.7.1/src/update/Updater.cpp#L176-L279 https://github.com/gitahed/gitahed/issues/662 https://www.vulncheck.com/advisories/gitahed-2.5.0-through-2.7.1-unverified-update-installation-and-tls-bypass	none	no	total
CVE-2026-105314	7,5	Papermerge	Path Traversal: '../filedir'	3.5.3	https://github.com/kashishtopi/cve-pocs/blob/main/papermerge-core-arbitrary-file-write-rce/HR-papermerge-core-path-traversal-rce.pdf https://github.com/kashishtopi/cve-pocs/tree/main/papermerge-core-arbitrary-file-write-rce https://github.com/papermerge/papermerge-core/blob/master/papermerge/core/features/document/router.py https://github.com/papermerge/papermerge-core/blob/master/papermerge/core/pathlib.py			
CVE-2026-105744	7,5	docling; docling-slim	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); External Control of File Name or Path; Initialization of a Resource with an Insecure Default	>= 2.94.0, < 2.132.0	https://github.com/docling-project/docling/commit/38b6fa0a465d46fdacbbe333f50fa19c4f6b342 https://github.com/docling-project/docling/pull/4419 https://github.com/docling-project/docling/releases/tag/v2.132.0 https://github.com/docling-project/docling/security/advisories/GHSA-x3q2-h9hx-4r4j			
CVE-2026-105782	7,5	Scrapy	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	>= 1.4.0, < 2.14.2	https://github.com/scrapy/scrapy/commit/945b787a263586cb5803c01c6da57daad8997ae5 https://github.com/scrapy/scrapy/commit/b6e5c58ae707a3d4bb491537b5519534050047e0 https://github.com/scrapy/scrapy/releases/tag/2.14.2 https://github.com/scrapy/scrapy/security/advisories/GHSA-cwxi-rr6w-m6w7			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-20519	7,5	In Modem, there	Out-of-bounds Write	MT2716; MT2735; MT2737; MT6813; MT6815; MT6833; MT6835; MT6853; MT6855; MT6858; MT6873; MT6875; MT6877; MT6878; MT6879; MT6880; MT6881; MT6883; MT6885; MT6886; MT6889; MT6890; MT6891; MT6893; MT6895; MT6896; MT6897; MT6899; MT6980; MT6982; MT6983; MT6985; MT6986; MT6988; MT6989; MT6990; MT6991; MT6993; MT8668; MT8676; MT8678; MT8695; MT8696; MT8755; MT8771; MT8775; MT8791; MT8791T; MT8792; MT8793; MT8796; MT8797; MT8798; MT8863; MT8873; MT8883; MT8893	https://www.mediatek.com/product-security-bulletin/October-2026	none	no	total
CVE-2026-39723	7,5	Morning for WooCommerce	Missing Authorization	<= 2.4.1	https://patchstack.com/database/wordpress/plugin/wc-gateway-greeninvoice/vulnerability/wordpress-morning-for-woocommerce-plugin-2-4-1-broken-access-control-vulnerability? s_id=cve			
CVE-2026-39789	7,5	Fluent Affiliate Pro	Missing Authorization	<= 1.6.4	https://patchstack.com/database/wordpress/plugin/fluent-affiliate-pro/vulnerability/wordpress-fluent-affiliate-pro-plugin-1-6-4-broken-access-control-vulnerability? s_id=cve			
CVE-2026-41558	7,5	WP Migration Plugin DB & Files – WP Synchro	Authentication Bypass by Spoofing	<= 1.16.1	https://patchstack.com/database/wordpress/plugin/wpsynchro/vulnerability/wordpress-wp-migration-plugin-db-files-wp-synchro-plugin-1-16-1-2fa-bypass-vulnerability? s_id=cve			
CVE-2026-41563	7,5	Sitemovr	Insertion of Sensitive Infor- mation Into Sent Data	<= 1.0.1	https://patchstack.com/database/wordpress/plugin/site-movr/vulnerability/wordpress-sitemovr-plugin-1-0-1-sensitive-data-exposure-vulnerability? s_id=cve			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-75028	7,5	The WPCafe – Restaurant Menu, Online Food Ordering & Table Booking System plugin for WordPress	Improper Control of File-name for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	up to, and including, 3.0.18	https://plugins.trac.wordpress.org/browser/wp-cafe/tags/3.0.17/core/shortcodes/views/food-menu/food-list.php#L53 https://plugins.trac.wordpress.org/browser/wp-cafe/tags/3.0.17/core/shortcodes/views/food-menu/food-list.php#L6 https://plugins.trac.wordpress.org/browser/wp-cafe/tags/3.0.17/core/shortcodes/views/food-menu/location-menu.php#L28 https://plugins.trac.wordpress.org/browser/wp-cafe/tags/3.0.17/widgets/wpc-food-location/wpc-food-location.php#L830 https://plugins.trac.wordpress.org/browser/wp-cafe/tags/3.0.17/widgets/wpc-food-menu-tab/wpc-food-menu-tab.php#L848 https://plugins.trac.wordpress.org/browser/wp-cafe/tags/3.0.17/widgets/wpc-location-menu/wpc-location-menu.php#L898	none	no	total
CVE-2026-88779	7,5	NetScaler ADC and NetScaler Gateway	Improper Restriction of Operations within the Bounds of a Memory Buffer	before 14.1-73.41; before 13.1-64.28; before 13.1-37.282; before 13.1-64.28.	https://community.citrix.com/techzone-blogs/110_security-updates/understanding-and-addressing-cve-2026-88779-in-citrix-netscaler-adc-and-citrix-netscaler-gateway/ https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174	active	yes	partial
CVE-2026-93428	7,5	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress	Missing Authorization	up to, and including, 2.13.1	https://github.com/ultimatemember/ultimatemember/releases/tag/2.14.0 https://plugins.trac.wordpress.org/browser/ultimate-member/tags/2.13.1/includes/core/class-ajax-common.php#L61 https://plugins.trac.wordpress.org/browser/ultimate-member/tags/2.13.1/includes/core/class-fields.php#L144 https://plugins.trac.wordpress.org/browser/ultimate-member/tags/2.13.1/includes/core/class-member-directory.php#L2795 https://plugins.trac.wordpress.org/browser/ultimate-member/tags/2.13.1/includes/core/class-member-directory.php#L2839 https://plugins.trac.wordpress.org/browser/ultimate-member/tags/2.13.1/includes/core/um-actions-profile.php#L1319	none	yes	partial
CVE-2026-96267	7,5	The WP Visitor Statistics (Real Time Traffic) plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 8.7	https://plugins.trac.wordpress.org/browser/wp-stats-manager/tags/8.6/includes/wsm_db.php#L1082 https://plugins.trac.wordpress.org/browser/wp-stats-manager/tags/8.6/includes/wsm_functions.php#L3091 https://plugins.trac.wordpress.org/browser/wp-stats-manager/tags/8.6/includes/wsm_requests.php#L140 https://plugins.trac.wordpress.org/browser/wp-stats-manager/tags/8.6/includes/wsm_statistics.php#L3252 https://plugins.trac.wordpress.org/browser/wp-stats-manager/tags/8.6/wp-stats-manager.php#L103 https://plugins.trac.wordpress.org/changelog?reponame=&old=3722831%40wp-stats-manager&new=3722831%40wp-stats-manager	none	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-97337	7,5	The Simple Membership plugin for WordPress	Missing Authorization	up to, and including, 4.8.3	https://plugins.trac.wordpress.org/browser/simple-membership/tags/4.8.3/classes/class.swpm-front-registration.php#L774 https://plugins.trac.wordpress.org/browser/simple-membership/tags/4.8.3/classes/class.swpm-front-registration.php#L850 https://plugins.trac.wordpress.org/browser/simple-membership/tags/4.8.3/classes/class.swpm-init-time-tasks.php#L167 https://plugins.trac.wordpress.org/browser/simple-membership/tags/4.8.3/classes/class.swpm-registration.php#L75 https://plugins.trac.wordpress.org/changeset?reponame=&old=3716437%40simple-membership&new=3716437%40simple-membership https://www.wordfence.com/threat-intel/vulnerabilities/id/ae2b6c4c-7dd6-41e7-8b8d-c09aa7fa660b?source=cve	none	yes	partial
CVE-2026-105222	7,4	The alexpechkarev/google-maps Laravel package	Improper Certificate Validation	through 12.16	https://github.com/alexpechkarev/google-maps https://github.com/alexpechkarev/google-maps/blob/v12.14/src/WebService.php#L267-L269 https://github.com/alexpechkarev/google-maps/blob/v12.16/src/config/googlemaps.php#L28 https://github.com/alexpechkarev/google-maps/issues/123 https://www.vulncheck.com/advisories/alexpechkarev-google-maps-through-12.16-disabled-tls-certificate-verification-via-ssl-verify-peer	none	no	total
CVE-2026-105223	7,4	kubernetes-client	Improper Certificate Validation	before 0.32.0	https://github.com/maclof/kubernetes-client https://github.com/maclof/kubernetes-client/blob/0.31.0/src/Client.php#L309-L312 https://github.com/maclof/kubernetes-client/commit/924c0b935fa538ed6b4b0948127609e99d0e6f34 https://github.com/maclof/kubernetes-client/issues/135 https://github.com/maclof/kubernetes-client/releases/tag/0.32.0 https://www.vulncheck.com/advisories/maclof-kubernetes-client-0.17.0-before-0.32.0-disabled-tls-certificate-verification	none	no	total
CVE-2026-105158	7,3	RainyGao DocSys	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to 2.02.85.	https://gitee.com/RainyGao/DocSys/ https://gitee.com/RainyGao/DocSys/issues/IK8NEU https://vuldb.com/cve/CVE-2026-105158 https://vuldb.com/submit/953425 https://vuldb.com/vuln/413377 https://vuldb.com/vuln/413377/ctj	poc	yes	partial
CVE-2026-105167	7,3	kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	411989e3ecb82895e53dca7865f72145f03d7d93; b3a70b2c492dc9904de5be1ad9389bd79b87f82c	https://github.com/kishor-23/food-waste-management-system/ https://github.com/kishor-23/food-waste-management-system/issues/7 https://vuldb.com/cve/CVE-2026-105167 https://vuldb.com/submit/970271 https://vuldb.com/vuln/413399 https://vuldb.com/vuln/413399/ctj	poc	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-105172	7,3	itsourcecode Online Admission System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/10RZC22/cve_submit/issues/1 https://itsourcecode.com/ https://vuldb.com/cve/CVE-2026-105172 https://vuldb.com/submit/970308 https://vuldb.com/vuln/413404 https://vuldb.com/vuln/413404/cti	poc	yes	partial
CVE-2026-105253	7,3	itsourcecode Online Admission System Project	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/marvhu821/Submit/issues/1 https://itsourcecode.com/ https://vuldb.com/cve/CVE-2026-105253 https://vuldb.com/submit/977177 https://vuldb.com/vuln/413462 https://vuldb.com/vuln/413462/cti	poc	yes	partial
CVE-2026-105571	7,3	PickMall Lilishop	Incorrect Privilege Assignment; Improper Authorization	up to 4.2.4.	https://github.com/lilishop/lilishop/issues/148 https://vuldb.com/cve/CVE-2026-105571 https://vuldb.com/submit/989282 https://vuldb.com/vuln/413630 https://vuldb.com/vuln/413630/cti			
CVE-2026-105776	7,3	bhagya3929 Employee-Movement-Tracking-and-Monitoring-Website-for-IOCL	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	ae783195ba7e0390d3b3bfadd99944b7e9735a4	https://github.com/bhagya3929/Employee-Movement-Tracking-and-Monitoring-Website-for-IOCL/ https://github.com/bhagya3929/Employee-Movement-Tracking-and-Monitoring-Website-for-IOCL/issues/1 https://vuldb.com/cve/CVE-2026-105776 https://vuldb.com/submit/992496 https://vuldb.com/vuln/413810 https://vuldb.com/vuln/413810/cti			
CVE-2026-101928	7,2	The Magic Tooltips For Contact Form	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.0.34	https://plugins.trac.wordpress.org/browser/magic-tooltips-for-contact-form-7/trunk/lib/wp-hooks.php#L96 https://plugins.trac.wordpress.org/browser/magic-tooltips-for-contact-form-7/trunk/magic-tooltips-for-contact-form-7.php#L18 https://plugins.trac.wordpress.org/changeset?reponame=&old=3723483%40magic-tooltips-for-contact-form-7&new=3723483%40magic-tooltips-for-contact-form-7 https://www.wordfence.com/threat-intel/vulnerabilities/id/94e8de22-c373-4f0c-9723-f19752ade4e7?source=cve	none	no	partial
CVE-2026-75962	7,2	Post SMTP – Complete Email Delivery and SMTP Solution with Email Logs, Alerts, Backup SMTP & Mobile App	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 4.0.1	https://plugins.trac.wordpress.org/browser/post-smtp/tags/3.9.5/Postman/Postman-Email-Log/PostmanEmailLogService.php#L215 https://plugins.trac.wordpress.org/browser/post-smtp/tags/3.9.5/Postman/Postman-Mail/PostmanEmailAddress.php#L63 https://plugins.trac.wordpress.org/browser/post-smtp/tags/3.9.5/Postman/PostmanEmailLogs.php#L538 https://plugins.trac.wordpress.org/browser/post-smtp/tags/3.9.5/Postman/PostmanWpMail.php#L374 https://plugins.trac.wordpress.org/browser/post-smtp/tags/3.9.5/script/postman-email-logs.js#L711 https://plugins.trac.wordpress.org/changeset/3711068/post-smtp/trunk/Postman/Postman-Email-Log/PostmanEmailLogService.php			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-87091	7,2	The Welcart e-Commerce plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.12.2	https://plugins.trac.wordpress.org/browser/usc-e-shop/tags/2.11.29/functions/hoock_func.php#L631 https://plugins.trac.wordpress.org/browser/usc-e-shop/tags/2.11.29/functions/settlement_func.php#L569 https://plugins.trac.wordpress.org/browser/usc-e-shop/tags/2.11.29/functions/settlement_func.php#L906 https://plugins.trac.wordpress.org/browser/usc-e-shop/tags/2.11.29/functions/settlement_func.php#L951 https://plugins.trac.wordpress.org/browser/usc-e-shop/tags/2.12.2/functions/hoock_func.php#L631 https://plugins.trac.wordpress.org/browser/usc-e-shop/tags/2.12.2/functions/settlement_func.php#L569	none	yes	partial
CVE-2026-92977	7,2	The Real Cookie Banner: GDPR & ePrivacy Cookie Consent plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 5.3.5	https://plugins.trac.wordpress.org/browser/real-cookie-banner/tags/5.3.0/inc/view/Blocker.php#L213 https://plugins.trac.wordpress.org/browser/real-cookie-banner/tags/5.3.0/inc/view/Blocker.php#L233 https://plugins.trac.wordpress.org/browser/real-cookie-banner/tags/5.3.0/vendor/devowl-wp/fast-html-tag/src/FastHtmlTag.php#L166 https://plugins.trac.wordpress.org/changeset?reponame=&old=3710645%40real-cookie-banner&new=3710645%40real-cookie-banner https://www.wordfence.com/threat-intel/vulnerabilities/id/32fba37-208c-4e94-8d07-f3fd14ee2ee1?source=cve	none	no	partial
CVE-2026-93430	7,2	The GD Rating System plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 3.7.1	https://plugins.trac.wordpress.org/browser/gd-rating-system/tags/3.7.1/rating/core.ajax.php#L184 https://plugins.trac.wordpress.org/browser/gd-rating-system/tags/3.7.1/rating/core.item.php#L383 https://plugins.trac.wordpress.org/browser/gd-rating-system/tags/3.7.1/rating/engine.single.php#L140 https://plugins.trac.wordpress.org/browser/gd-rating-system/tags/3.7.1/templates/stars-rating/qdrt--stars-rating--list--default-table.php#L44 https://plugins.trac.wordpress.org/changeset?reponame=&old=3723329%40gd-rating-system&new=3723329%40gd-rating-system https://www.wordfence.com/threat-intel/vulnerabilities/id/5f06140d-c28f-4dfb-be61-cc8f59884766?source=cve	none	no	partial
CVE-2026-93889	7,2	The Mail logging – WP Mail Catcher plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.1.12	https://plugins.trac.wordpress.org/browser/wp-mail-catcher/tags/2.1.12/src/Loggers/LogHelper.php#L69 https://plugins.trac.wordpress.org/browser/wp-mail-catcher/tags/2.1.12/src/Loggers/WpMail.php#L30 https://plugins.trac.wordpress.org/browser/wp-mail-catcher/tags/2.1.12/src/MailAdminTable.php#L149 https://plugins.trac.wordpress.org/browser/wp-mail-catcher/tags/2.1.12/src/Views/LogModal.php#L83 https://plugins.trac.wordpress.org/changeset?reponame=&old=3717442%40wp-mail-catcher&new=3717442%40wp-mail-catcher https://www.wordfence.com/threat-intel/vulnerabilities/id/6a1d9d03-0216-484c-85ca-73f157595713?source=cve	none	no	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-96564	7,2	The SEOPress – AI SEO Plugin & On-site SEO plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 10.2	https://plugins.trac.wordpress.org/browser/wp-seopress/tags/10.2/inc/functions/options-google-analytics.php#L635 https://plugins.trac.wordpress.org/browser/wp-seopress/tags/10.2/inc/functions/options-matomo.php#L118 https://plugins.trac.wordpress.org/changeset?reponame=&old=3722789%40wp-seopress&new=3722789%40wp-seopress https://www.wordfence.com/threat-intel/vulnerabilities/id/8f5f5b75-abaf-4e4b-8509-f8b569519166?source=cve	none	yes	partial
CVE-2026-96575	7,2	The Transliterator – Multilingual and Multi-script Text Conversion plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.5.8	https://plugins.trac.wordpress.org/browser/serbian-transliteration/tags/2.5.8/classes/controller.php#L659 https://plugins.trac.wordpress.org/browser/serbian-transliteration/tags/2.5.8/classes/controller.php#L679 https://plugins.trac.wordpress.org/browser/serbian-transliteration/tags/2.5.8/classes/controller.php#L689 https://plugins.trac.wordpress.org/changeset?reponame=&old=3714692%40serbian-transliteration&new=3714692%40serbian-transliteration https://www.wordfence.com/threat-intel/vulnerabilities/id/31bf520-2006-496b-b487-62faea679cf6?source=cve	none	no	partial
CVE-2026-96650	7,2	The Strong Testimonials plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 3.3.11	https://plugins.trac.wordpress.org/browser/strong-testimonials/tags/3.3.10/includes/class-strong-testimonials-form.php#L260 https://plugins.trac.wordpress.org/browser/strong-testimonials/tags/3.3.10/includes/class-strong-testimonials-form.php#L32 https://plugins.trac.wordpress.org/browser/strong-testimonials/tags/3.3.10/includes/functions-image.php#L242 https://plugins.trac.wordpress.org/browser/strong-testimonials/tags/3.3.10/includes/functions-image.php#L275 https://plugins.trac.wordpress.org/changeset?reponame=&old=3711376%40strong-testimonials&new=3711376%40strong-testimonials https://www.wordfence.com/threat-intel/vulnerabilities/id/73c8267c-8c03-4ee6-9d3e-e383188b82ad?source=cve	none	no	partial
CVE-2026-97341	7,2	The Visitor Traffic Real Time Statistics plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 8.16	https://plugins.trac.wordpress.org/browser/visitors-traffic-real-time-statistics/tags/8.14/WPHitsCounter.php#L877 https://plugins.trac.wordpress.org/browser/visitors-traffic-real-time-statistics/tags/8.14/functions.php#L3407 https://plugins.trac.wordpress.org/browser/visitors-traffic-real-time-statistics/tags/8.14/functions.php#L3756 https://plugins.trac.wordpress.org/browser/visitors-traffic-real-time-statistics/tags/8.14/functions.php#L4735 https://plugins.trac.wordpress.org/browser/visitors-traffic-real-time-statistics/tags/8.14/js/ahcfree_js_scripts.js#L1036 https://plugins.trac.wordpress.org/changeset?reponame=&old=3722792%40visitors-traffic-real-time-statistics&new=3722792%40visitors-traffic-real-time-statistics	none	no	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-97660	7,2	The WPC Product Options for WooCommerce plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 4.0.5	https://plugins.trac.wordpress.org/browser/wpc-product-options/tags/4.0.5/includes/class-cart.php#L336 https://plugins.trac.wordpress.org/browser/wpc-product-options/tags/4.0.5/includes/class-cart.php#L537 https://plugins.trac.wordpress.org/browser/wpc-product-options/tags/4.0.5/includes/class-cart.php#L573 https://plugins.trac.wordpress.org/browser/wpc-product-options/tags/4.0.5/includes/class-cart.php#L579 https://plugins.trac.wordpress.org/browser/wpc-product-options/tags/4.0.5/includes/class-cart.php#L792 https://plugins.trac.wordpress.org/changeset?reponame=&old=3712354%40wpc-product-options&new=3712354%40wpc-product-options	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
CISA Adds One Known Exploited Vulnerability to Catalog CISA	CVE-2026-88779 Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability	https://cisa.gov/news-events/alerts/2026/10/04/cisa-adds-one-known-exploited-vulnerability-catalog

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
FBI Removes Accenture Contractor After Patch Failure Led to Shiny-Hunters Breach	https://thehackernews.com/2026/10/fbi-removes-accenture-contractor-after.html
OpenAI is adding invisible watermarks to ChatGPT and Codex text in the EU	https://bleepingcomputer.com/news/artificial-intelligence/openai-is-adding-invisible-watermarks-to-chatgpt-and-codex-text-in-the-eu
IQVIA fined \$7.8 million for failing to properly anonymize health data	https://bleepingcomputer.com/news/security/iqvia-fined-78-million-for-failing-to-properly-anonymize-health-data

16 Suspects Detained in Timor-Leste for Japanese Police Impersonation Scam	https://cybersecuritynews.com/timor-leste
Google Narrows Open Source Bug Bounty Amid Wave of Invalid Automated Reports	https://securityweek.com/google-narrows-open-source-bug-bounty-amid-wave-of-invalid-automated-reports
South Korea probes bank breaches amid suspected AI-powered attacks	https://bleepingcomputer.com/news/security/south-korea-probes-bank-breaches-amid-suspected-ai-powered-attacks
Researcher Infiltrates Lazarus Group's Crypto Laundering Network After \$1.5B Bybit Hack	https://cybersecuritynews.com/zachxbt-infiltrates-lazarus-group
Linux Backdoors Target Telecoms, Masquerade as Email Traffic	https://infosecurity-magazine.com/news/smtp-linux-backdoors-network-edge
Google Gemini Will Soon Get Full Access Permission to Use Your Computer	https://cybersecuritynews.com/google-gemini-computer-access
Citrix NetScaler Targeted Via New Zero Day	https://infosecurity-magazine.com/news/citrix-netscaler-zero-day
RemoveMacAI Free Up 12GB of Data by Removing Apple Intelligence Models	https://cybersecuritynews.com/removemacai-removes-ai-models
250,000 Impacted by Data Breaches at New Jersey, Texas Healthcare Firms	https://securityweek.com/250000-impacted-by-data-breaches-at-new-jersey-texas-healthcare-firms
Senate Passes Bipartisan Bill to Strengthen Healthcare Cybersecurity	https://securityweek.com/senate-passes-bipartisan-bill-to-strengthen-healthcare-cybersecurity
Apple Plans Tighter macOS Full Disk Access Controls Over AI Agent Data Access	https://thehackernews.com/2026/10/apple-plans-tighter-macos-full-disk.html
OpenAI will show visual ads in ChatGPT while you generate images	https://bleepingcomputer.com/news/artificial-intelligence/openai-will-show-visual-ads-in-chatgpt-while-you-generate-images
Privacy Policy	https://cybersecuritynews.com/privacy-policy-2
Article Publication and Retention Policy	https://cybersecuritynews.com/terms-of-service
About Us	https://cybersecuritynews.com/about-us
Microsoft: Windows KB5124010 update crashes some games and apps	https://bleepingcomputer.com/news/microsoft/microsoft-windows-kb5124010-update-crashes-some-games-and-apps
More UK Schools Are Recovering Faster from Cyber Incidents	https://infosecurity-magazine.com/news/uk-schools-recovering-faster

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
Denmark population registry data breach affects 8.8 million people	https://bleepingcomputer.com/news/security/denmark-population-registry-data-breach-affects-88-million-people
Denmark Data Breach Exposes Personal Records of 8.8 Million People	https://cybersecuritynews.com/denmark-data-breach
Frontline Education Breach Impacts K-12 School District Staff	https://infosecurity-magazine.com/news/frontline-education-breach-k12
Cybersecurity Newsletter Bulletin – Pentagon Data Breach, Citrix, Forti-mail and Apple 0-days and 20+ stories	https://cybersecuritynews.com/cybersecurity-newsletter-weekly-october-2

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 Atlassian Flaw Lets Unauthenticated Attackers Read Known Files Across 8 Products	https://thehackernews.com/2026/10/critical-atlassian-flaw-lets.html
Rejetto HFS servers now actively scanned for critical RCE flaw	https://bleepingcomputer.com/news/security/rejetto-hfs-servers-now-actively-scanned-for-critical-rce-flaw
Microsoft Exchange Flaw Lets Authenticated Attackers Read Other Users' Mailboxes	https://thehackernews.com/2026/10/microsoft-exchange-flaw-lets.html
Malicious HEIC Images Can Trigger Remote Code Execution on WordPress Servers	https://cybersecuritynews.com/malicious-heic-images
New Dell System Update flaw lets hackers gain root privileges	https://bleepingcomputer.com/news/security/new-dell-system-update-flaw-lets-hackers-gain-root-privileges
Zammad Zero-Day Chain Lets AI Agent Hijack Sessions, Execute Code and Escalate to Root	https://cybersecuritynews.com/zammad-zero-day
CISA Warns of Citrix NetScaler Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/cisa-citrix-netscaler-vulnerability-exploited
Exploitation Hits Rejetto HFS Vulnerability Discovered by AI	https://securityweek.com/exploitation-hits-rejetto-hfs-vulnerability-discovered-by-ai
Google Suspends Open-Source Bug Bounty Due to AI Vulnerability Reports	https://infosecurity-magazine.com/news/google-suspends-opensource-bug
CISA Adds Fortinet FortiMail 0-day Vulnerability to KEV Following Active Exploitation	https://cybersecuritynews.com/fortinet-fortimail-0-day-vulnerability-exploitation
Attackers Target Rejetto HFS Flaw That Enables Admin Session Forgery and RCE	https://thehackernews.com/2026/10/attackers-target-rejetto-hfs-flaw-that.html
New NetScaler Zero-Day Exploited in Targeted Attacks Can Knock SAML Deployments Offline	https://thehackernews.com/2026/10/new-netscaler-zero-day-exploited-in.html
Exploitation of Citrix NetScaler Zero-Day Hits Appliances Patched Days Earlier	https://securityweek.com/exploitation-of-citrix-netscaler-zero-day-hits-appliances-patched-days-earlier
Citrix NetScaler SAML 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/citrix-netscaler-saml-0-day-vulnerability
Vercel Confirms KVM Zero-Day VM Escape, Awards Researcher \$50,000	https://cybersecuritynews.com/kvm-zero-day-vm-escape
Microsoft Pushes New Exchange V2 Update After Discovering New Security Flaw	https://cybersecuritynews.com/microsoft-reissues-exchange-server-update
Critical GitLab AI Gateway Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/gitlab-ai-gateway-vulnerability
Citrix NetScaler Keeps Rebooting Following the 0-Day Patch	https://cybersecuritynews.com/citrix-netscaler-0-day-patch

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
ClingSTUN Malware Turns Unpatched IoT Devices Into Proxy Nodes	https://infosecurity-magazine.com/news/clingstun-backdoor-unpatched-iot
Citrix patches NetScaler SAML zero-day exploited in attacks	https://bleepingcomputer.com/news/security/citrix-patches-netscaler-saml-zero-day-exploited-in-attacks
Fortra Patches Critical Vulnerabilities in BoKS	https://securityweek.com/fortra-patches-critical-vulnerabilities-in-boks

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
⚡ Weekly Recap: NetScaler and FortiMail 0-Days, AI Coding Leaks, Spectre v2 and Ransomware Arrests	https://thehackernews.com/2026/10/weekly-recap-netscaler-and-fortimail-0.html
ClickFix Fake CAPTCHA Attack Executes Malware Hidden Inside Browser Cache	https://cybersecuritynews.com/clickfix-fake-captcha-attack
Alleged dev of Ploutus ATM malware appears in US court after arrest	https://bleepingcomputer.com/news/security/suspected-dev-of-ploutus-atm-malware-appears-in-us-court-after-arrest
Linux Backdoor Abuses STUN Protocol, Exploits Dozens of Flaws	https://securityweek.com/linux-backdoor-abuses-stun-protocol-exploits-dozens-of-flaws
GlassWorm Supply Chain Attack Uses Fake VS Code Themes to Deliver Hidden Malware	https://cybersecuritynews.com/glassworm-supply-chain-attack
Realtek Jungle SDK Exploit Attempts Deliver Cling Botnet With STUN-Based C2	https://thehackernews.com/2026/10/realtek-jungle-sdk-exploit-attempts.html
Hackers Abuse Legitimate ScreenConnect Tool to Gain Remote Access Through Phishing	https://cybersecuritynews.com/screenconnect-tool
Warlock Exploits SharePoint Flaws to Disable Security Tools and Deploy Ransomware	https://thehackernews.com/2026/10/warlock-exploits-sharepoint-flaws-to.html

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
Top 10 Best Just-in-Time (JIT) Access Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-jit-access-tools

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 ≥ 7.0 , αφορούν το διάστημα 03/10/2026–06/10/2026, 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 https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ Scan your WordPress website, https://wpscan.com/scan/
Oracle	Critical Patch Updates, Security Alerts and Bulletins, https://www.oracle.com/security-alerts/
Fortinet	Fortinet products, https://www.fortiguard.com/psirt
IBM	Security bulletins, https://cloud.ibm.com/status/security Research, Collaborate and Act on threat intelligence, https://exchange.xforce.ibmcloud.com/
MS Windows	The Microsoft Security Response Center (MSRC), https://msrc.microsoft.com/update-guide/
SAP	SAP Security Notes, https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
Dell	Security Advisories, Notices and Resources, https://www.dell.com/support/security/en-us
HPE	HPE Security Bulletin Library, https://support.hpe.com/connect/s/securitybulletinlibrary Security Bulletins, https://support.hp.com/us-en/security-bulletins
Cisco	Cisco Security Advisories, https://sec.cloudapps.cisco.com/security/center/publicationListing.x
Palo Alto	Palo Alto Networks Security Advisories, https://security.paloaltonetworks.com/
Ivanti	Security Advisory, https://www.ivanti.com/blog/topics/security-advisory
Mozilla	Mozilla Foundation Security Advisories, https://www.mozilla.org/en-US/security/advisories/
Android	Android Security Bulletins, https://source.android.com/docs/security/bulletin/asb-overview
Zyxel	Security Advisories, https://www.zyxel.com/global/en/support/security-advisories
D-Link	Global Security Advisories, Responses, and Notices, https://supportannouncement.us.dlink.com/
Adobe	Security Bulletins and Advisories, https://helpx.adobe.com/security/security-bulletin.html
Siemens	Siemens ProductCERT and Siemens CERT, https://www.siemens.com/global/en/products/services/cert.html
Splunk	Splunk Security Advisories, https://advisory.splunk.com/