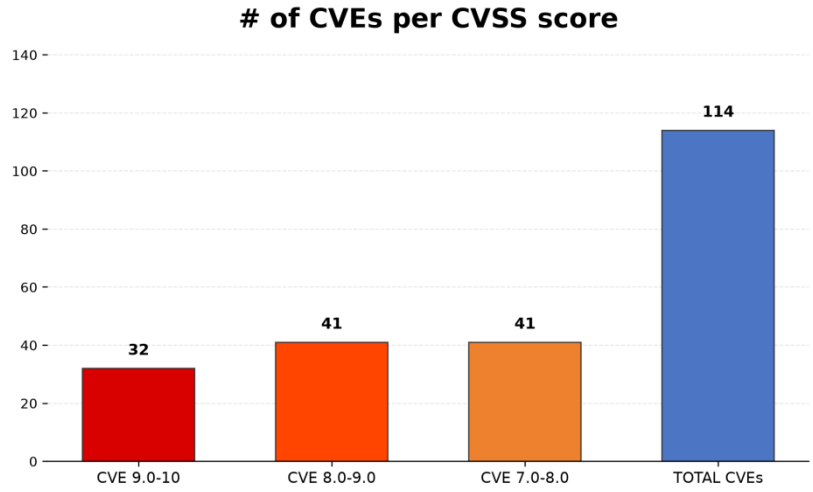
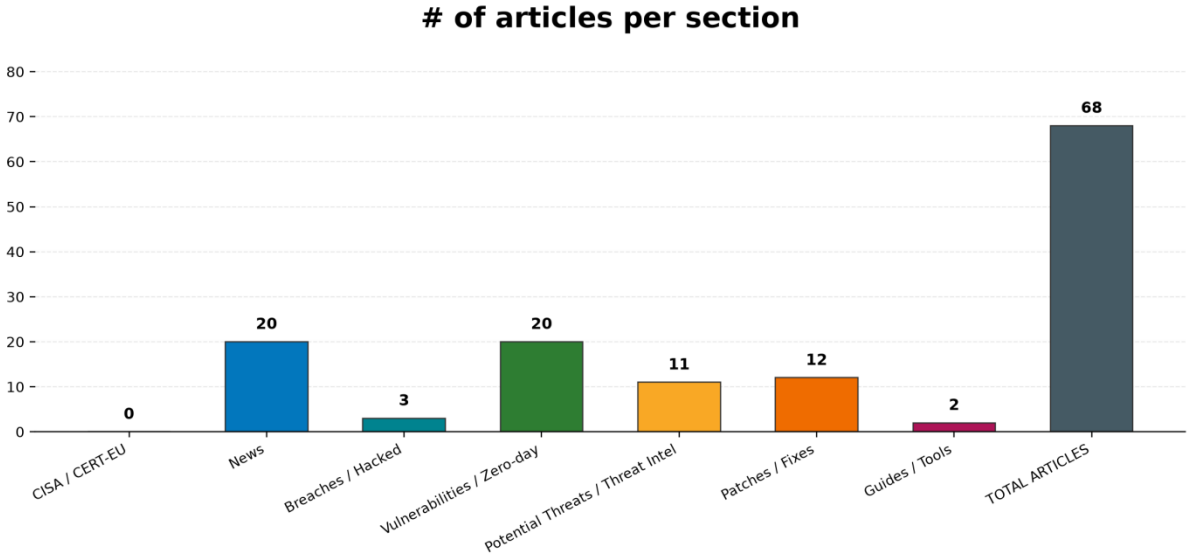
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 12/08/2026 - 14/08/2026





Contents

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-2026-15413	10,0	The Link Factory WordPress plugin	Hidden Functionality		https://wpscan.com/vulnerability/4cad269d-0146-4ca9-a1ae-55f02c8e5433/	none	yes	total
CVE-2026-27544	10,0	QA Analytics	Improper Control of Generation of Code ('Code Injection')	<= 5.2.0.0	https://patchstack.com/database/wordpress/plugin/qa-heatmap-analytics/vulnerability/wordpress-qa-analytics-plugin-5-2-0-0-remote-code-execution-rce-vulnerability?_s_id=cve	none	yes	total
CVE-2026-59500	10,0	Portal Generator addon to Priority ERP (developed by Soft Solutions)	Improper Authentication	All versions without Priwall v3	https://www.gov.il/en/departments/dynamiccollectors/cve_advisories_listing?skip=0	none	yes	total
CVE-2026-61962	10,0	WP BASE Booking	Improper Control of Generation of Code ('Code Injection')	<= 6.3.0	https://patchstack.com/database/wordpress/plugin/wp-base-booking-of-appointments-services-and-events/vulnerability/wordpress-wp-base-booking-plugin-6-3-0-arbitrary-code-execution-vulnerability?_s_id=cve	none	yes	total
CVE-2026-72851	10,0	Budibase	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 3.40.0	https://github.com/Budibase/budibase/security/advisories/GHSA-x7h8-ww3q-xv7c https://www.vulncheck.com/advisories/budibase-before-sql-injection-via-unauthenticated-webhook			
CVE-2026-73299	10,0	Prompty	Improper Control of Generation of Code ('Code Injection'); Improper Neutralization of Special Elements Used in a Template Engine	Prior to 0.1.5 and 2.0.0-beta.5	https://github.com/microsoft/prompty/commit/e4a0ebf49e3a78d5d7796c8480bf9a4f0c54d19e https://github.com/microsoft/prompty/commit/f5c57c94a0990cca79d095c3daab661b4b1fb89f https://github.com/microsoft/prompty/pull/404 https://github.com/microsoft/prompty/pull/405 https://github.com/microsoft/prompty/security/advisories/GHSA-w28w-gp39-m4p6 https://github.com/microsoft/prompty/tree/typescript/2.0.0-beta.5	none	yes	total
CVE-2026-63297	9,9	LXD due to a timing flaw during configuration merging	Time-of-check Time-of-use (TOCTOU) Race Condition; Incorrect Authorization	5.0.0 prior to 5.0.8; 5.21.0 prior to 5.21.6	https://github.com/canonical/lxd/security/advisories/GHSA-v989-gw7w-xvg4	poc	no	total
CVE-2026-63298	9,9	LXD's NVIDIA instance configuration handling	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	5.0.0 prior to 5.0.8; 5.21.0 prior to 5.21.6; 4.0.0 prior to 4.0.12	https://github.com/canonical/lxd/security/advisories/GHSA-vfh7-q59g-54v2	poc	no	total
CVE-2026-63300	9,9	the instance-PostMigration function in lxd/instance_post	Missing Authorization	5.0.0 prior to 5.0.8; 5.21.0 prior to 5.21.6; 6.0 prior to 6.10	https://github.com/canonical/lxd/pull/18605 https://github.com/canonical/lxd/pull/18651 https://github.com/canonical/lxd/security/advisories/GHSA-5q5r-wh97-qcq2	poc	no	total
CVE-2026-72841	9,9	luci	External Control of File Name or Path		https://github.com/openwrt/luci/security/advisories/GHSA-jjcx-c284-2qv8 https://www.vulncheck.com/advisories/luci-app-openvpn-path-traversal-rce-via-instance-name2			
CVE-2026-72842	9,9	luci-app-lxc	External Control of File Name or Path		https://github.com/openwrt/luci/security/advisories/GHSA-jf59-v86x-fwf2 https://www.vulncheck.com/advisories/openwrt-luci-app-lxc-acl-inconsistency-authentication-bypass			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-73263	9,9	Prowler	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 5.36.0	https://github.com/prowler-cloud/prowler/commit/0b782fcb8c24ece7bd38deede2b8f13d8583e39c https://github.com/prowler-cloud/prowler/pull/12091 https://github.com/prowler-cloud/prowler/releases/tag/5.36.0 https://github.com/prowler-cloud/prowler/security/advisories/GHSA-ccqh-6cjc-wp4j	none	no	total
CVE-2026-73656	9,9	trigger.dev	Authorization Bypass Through User-Controlled Key; Missing Authorization	Prior to 4.5.6	https://github.com/triggerdotdev/trigger.dev/commit/34b1a181c2a1d33a53ebab88f84b05f81fea4254 https://github.com/triggerdotdev/trigger.dev/pull/4199 https://github.com/triggerdotdev/trigger.dev/releases/tag/v4.5.2 https://github.com/triggerdotdev/trigger.dev/security/advisories/GHSA-j6vv-pg9h-f4wj			
CVE-2026-14182	9,8	The Customer Email Verification for WooCommerce WordPress plugin	Improper Authentication	before 3.2.6	https://wpscan.com/vulnerability/ef4e95a3-6f90-4423-9551-9ac28f7b6291/	none	yes	total
CVE-2026-15039	9,8	The giftware WordPress plugin	Unrestricted Upload of File with Dangerous Type	before 4.2.10	https://wpscan.com/vulnerability/b7b3308c-430e-4bc3-a3df-da20d47cf314/	poc	yes	total
CVE-2026-16051	9,8	The wpmudev-updates WordPress plugin	Improper Control of Generation of Code ('Code Injection')	before 5.0.1	https://wpscan.com/vulnerability/8dae5fbf-2e9d-4978-b97d-a20e076cd309/	poc	yes	total
CVE-2026-16770	9,8	PDF::WebKit versions	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	through 1.2	https://github.com/kingpong/perl-PDF-WebKit/issues/9 https://security.metacpan.org/patches/P/PDF-WebKit/1.2/CVE-2026-16770-r1.patch https://wkhtmltopdf.org/status.html http://www.openwall.com/lists/oss-security/2026/08/13/2	none	yes	total
CVE-2026-18366	9,8	The Events Manager WordPress plugin	Improper Privilege Management	before 7.4.1	https://wpscan.com/vulnerability/82767ce2-01e4-46ad-a52b-72d3ab2049bd/	poc	yes	total
CVE-2026-18391	9,8	The WooCommerce Subscriptions WordPress plugin	Unrestricted Upload of File with Dangerous Type	before 9.1.0	https://wpscan.com/vulnerability/191f76cf-e5bd-4a37-ac1c-9187cea2aa27/	poc	yes	total
CVE-2026-26035	9,8	Fortinet FortiWeb	Improper Authentication	8.0.0 through 8.0.2; 7.6.0 through 7.6.6; 7.4.0 through 7.4.11; 7.2.0 through 7.2.12; 7.0.0 through 7.0.12	https://fortiguard.fortinet.com/psirt/FG-IR-26-158	none	yes	total
CVE-2026-28008	9,8	OAuth Single Sign On – SSO (OAuth Client)	Authentication Bypass by Spoofing	<= 7.0.0	https://patchstack.com/database/wordpress/plugin/miniorange-login-with-eve-online-google-facebook/vulnerability/wordpress-oauth-single-sign-on-sso-oauth-client-plugin-7-0-0-broken-authentication-vulnerability?_s_id=cve	none	yes	total
CVE-2026-28185	9,8	Log in with Google	Insufficient Verification of Data Authenticity	<= 1.4.2	https://patchstack.com/database/wordpress/plugin/login-with-google/vulnerability/wordpress-log-in-with-google-plugin-1-4-2-broken-authentication-vulnerability?_s_id=cve	none	yes	total
CVE-2026-72839	9,8	filebrowser	Incorrect Privilege Assignment	through 2.63.16	https://github.com/filebrowser/filebrowser/security/advisories/GHSA-6759-996p-qpj6 https://www.vulncheck.com/advisories/filebrowser-through-privilege-escalation-via-signup			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-73644	9,6	OpenDJ	Improper Authorization; Authorization Bypass Through User-Controlled Key	Prior to 5.1.2	https://github.com/OpenIdentityPlatform/OpenDJ/commit/5c326850f1ab945cfca7ac9c5aaf77d1052c6bed https://github.com/OpenIdentityPlatform/OpenDJ/releases/tag/5.1.2 https://github.com/OpenIdentityPlatform/OpenDJ/security/advisories/GHSA-p279-2cgp-84jg			
CVE-2026-73843	9,6	OpenChoreo	Missing Authentication for Critical Function; Exposure of Resource to Wrong Sphere; Missing Authorization	Prior to 1.0.2 and 1.1.2	https://github.com/openchoreo/openchoreo/commit/047d80ddc63b4b4b9dd67044d5cffcdbd77685ce https://github.com/openchoreo/openchoreo/commit/0aa0ffe1623bd8eb4235cb2a5854336695953c3a https://github.com/openchoreo/openchoreo/commit/b42eeb0f5dce95195a9781d7c5a1fe9e38f5da8f https://github.com/openchoreo/openchoreo/pull/4122 https://github.com/openchoreo/openchoreo/releases/tag/v1.0.2 https://github.com/openchoreo/openchoreo/releases/tag/v1.1.2			
CVE-2026-8715	9,6	Vault Secrets Operator	Files or Directories Accessible to External Parties	up to 1.4.1	https://discuss.hashicorp.com/t/hcsec-2026-28-vault-secrets-operator-vulnerable-to-arbitrary-file-read-via-approle-secretidpath/77645	none	no	total
CVE-2026-66147	9,4	the GMS Dispatcher Service in GMS	Improper Control of Generation of Code ('Code Injection')	9.5.1 and earlier	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0011	none	yes	total
CVE-2026-73296	9,4	UFO	Missing Authentication for Critical Function; Missing Authorization	Prior to 3.0.8	https://github.com/microsoft/UFO/commit/e562d10060b077dedae93e0fd58c1ee379558962 https://github.com/microsoft/UFO/releases/tag/v3.0.8 https://github.com/microsoft/UFO/security/advisories/GHSA-24fq-m9rr-g3mm	poc	yes	total
CVE-2026-16538	9,1	The Wallet for WooCommerce WordPress plugin	Improper Access Control	before 1.6.10	https://wpscan.com/vulnerability/bc87bb91-a0c4-4d35-8be1-6d3ec2623a86/	poc	yes	total
CVE-2026-67568	9,1	The distributed Mira Android APK	Use of Hard-coded Credentials	1.7.1.47; 4.5.15.4	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsma-26-223-01.json https://www.cisa.gov/news-events/ics-medical-advisories/icsma-26-223-01	none	yes	total
CVE-2026-68431	9,1	Linux		368ba06881c395f1c9a7ba22203cf8d78b4addc0 prior to b62c510f59803f82f9b4c76ead2a56833b2984c7; 368ba06881c395f1c9a7ba22203cf8d78b4addc0 prior to cfc0b8e5080aec87700774e8568765eaa4b7b92b; df3a4518aee64f21bcafa891105b468413f27431; 543c12c2644e772caa6880662c2a852cfdc5a10c; e9cb7be2fcbaee9e808b729e92948d38d52e5add; 5.15.145 prior to 5.16; 6.1.34 prior to 6.2; 6.3.8 prior to 6.4; 6.4	https://git.kernel.org/stable/c/b62c510f59803f82f9b4c76ead2a56833b2984c7 https://git.kernel.org/stable/c/cfc0b8e5080aec87700774e8568765eaa4b7b92b			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-73567	9,1	sm-crypto	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	Prior to 0.5.0	https://github.com/JuneAndGreen/sm-crypto/commit/1f9bd7bd160c24efd9c26c8f7fda997c68c823d0 https://github.com/JuneAndGreen/sm-crypto/security/advisories/GHSA-vh45-f885-3848			
CVE-2026-57858	8,9	Cal.com Self-Hosted (Cal.diy)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	versions 2.1.1 through 6.2.0	https://ashtonr.com/blog/cve-2026-57858/ https://github.com/calcom/cal.com https://www.vulncheck.com/advisories/cal-com-cal-diy-stored-xss-via-bookingpagetagmanager-analytics-tracking-id	poc	no	total
CVE-2026-13613	8,8	The KiviCare WordPress plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 4.5.2	https://wpscan.com/vulnerability/76b7d66f-6fa3-41e1-9216-ec125e34ade9/	poc	no	total
CVE-2026-14662	8,8	PostgreSQL tsvector and tsquery data type functions	Integer Overflow or Wraparound	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-14662/	none	no	total
CVE-2026-14664	8,8	PostgreSQL regexp	Heap-based Buffer Overflow	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-14664/	none	no	total
CVE-2026-14669	8,8	PostgreSQL to_char(timestamptz)	Heap-based Buffer Overflow	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-14669/	none	no	total
CVE-2026-14670	8,8	PostgreSQL plperl return of a tied hash	Heap-based Buffer Overflow	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-14670/	none	no	total
CVE-2026-14671	8,8	PostgreSQL module "refint"	Access of Resource Using Incompatible Type ('Type Confusion')	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-14671/	none	no	total
CVE-2026-14676	8,8	PostgreSQL pg_stat_statements	Heap-based Buffer Overflow	18 prior to 18.5	https://www.postgresql.org/support/security/CVE-2026-14676/	none	no	total
CVE-2026-14677	8,8	Integer wraparound in PostgreSQL; PostgreSQL 32-bit builds of pltcl and plperl	Integer Overflow or Wraparound	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-14677/	none	no	total
CVE-2026-14680	8,8	Type confusion with PostgreSQL "internal" data type arguments	Access of Resource Using Incompatible Type ('Type Confusion')	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-14680/	none	no	total
CVE-2026-15741	8,8	PostgreSQL EXTRACT() deparse	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-15741/	none	no	total
CVE-2026-15742	8,8	PostgreSQL fuzzystrmatch	Integer Overflow or Wraparound	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-15742/	none	no	total
CVE-2026-16238	8,8	PostgreSQL pg_restore_attribute_stats()	Access of Resource Using Incompatible Type ('Type Confusion')	18 prior to 18.5	https://www.postgresql.org/support/security/CVE-2026-16238/	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-2026-16239	8,8	PostgreSQL "portal"/cursor lifecycle	Access of Resource Using Incompatible Type ('Type Confusion')	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-16239/	none	no	total
CVE-2026-18408	8,8	pg_dump in PostgreSQL	Inclusion of Functionality from Untrusted Control Sphere	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-18408/	none	no	total
CVE-2026-19385	8,8	PostgreSQL pg_dump of long function transform lists	Heap-based Buffer Overflow	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-19385/	none	no	total
CVE-2026-19556	8,8	V8 in Google Chrome	Use After Free	prior to 151.0.7922.137	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01815628406.html https://issues.chromium.org/issues/535000102	none	no	total
CVE-2026-19559	8,8	HTML in Google Chrome	Use After Free	prior to 151.0.7922.137	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01815628406.html https://issues.chromium.org/issues/540100588	none	no	total
CVE-2026-19560	8,8	Blink in Google Chrome	Use After Free	prior to 151.0.7922.137	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01815628406.html https://issues.chromium.org/issues/540482895	none	no	total
CVE-2026-55676	8,8	Malcolm	Unrestricted Upload of File with Dangerous Type	Prior to version 26.06.1	https://github.com/cisagov/Malcolm/releases/tag/v26.06.1 https://github.com/cisagov/Malcolm/security/advisories/GHSA-8cvp-m7pg-grp7	none	no	total
CVE-2026-66875	8,8	Mira Firmware; Mira Android App	Missing Authentication for Critical Function	1.7.1.47; 4.5.15.4	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsma-26-223-01.json https://www.cisa.gov/news-events/ics-medical-advisories/icsma-26-223-01	none	no	total
CVE-2026-72642	8,8	The native inference process that Elasticsearch	Use of Out-of-range Pointer Offset	8.19.0 through 8.19.19; 9.4.0 through 9.4.4; 9.5.0	https://discuss.elastic.co/t/elasticsearch-8-19-20-9-4-5-9-5-1-security-update-esa-2026-123/389504	none	no	total
CVE-2026-72840	8,8	OpenWrt LuCI; luci-mod-system-mounts that grants write access to /etc/crontabs/root to users intended only for mount configuration	Incorrect Privilege Assignment		https://github.com/openwrt/luci/security/advisories/GHSA-v5f9-62c7-cw29 https://www.vulncheck.com/advisories/openwrt-luci-luci-mod-system-mounts-acl-root-rce-via-crontab-write			
CVE-2026-73514	8,8	The address_standardizer extension for PostGIS	Out-of-bounds Write	through 3.7.0	https://github.com/postgis/address_standardizer/commit/423570b0dbf6cd9f6fc36de28a636e7b6e9aa8aa https://github.com/postgis/address_standardizer/pull/3 https://github.com/postgis/address_standardizer/pull/4 https://mehmetince.net/part-1-6-systemic-risks-in-the-managed-postgresql-industry-extension-risks-are-real-exploiting-postgis-memory-corruption-bug-at-neondb-supabase-and-many-more/ https://www.vulncheck.com/advisories/postgis-address-standardizer-out-of-bounds-write-via-standardize-address	poc	no	total
CVE-2026-15216	8,7	GitLab CE/EE affecting all	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18; before 19.0.6, 19.1; before 19.1.4; before 19.2.2	https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-2-released/ https://gitlab.com/gitlab-org/gitlab/-/work_items/605448 https://hackerone.com/reports/3830061	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-2026-49478	8,7	Fulcio	Server-Side Request Forgery (SSRF)	through 1.8.5	https://github.com/sigstore/fulcio/commit/378c654f48c3bafdced04ead7010aab2cb4c6ca1 https://github.com/sigstore/fulcio/pull/2354 https://github.com/sigstore/fulcio/releases/tag/v1.8.6 https://github.com/sigstore/fulcio/security/advisories/GHSA-f5mr-q85p-6hh6			
CVE-2026-72777	8,6	next-ai-draw-io	Server-Side Request Forgery (SSRF)	through 0.4.16	https://github.com/DayuanJiang/next-ai-draw-io/issues/918 https://www.vulncheck.com/advisories/next-ai-draw-io-ssrf-via-dns-rebinding-in-parse-url	poc	yes	partial
CVE-2026-73247	8,6	Kestra	Server-Side Request Forgery (SSRF)	Prior to 2.0.0	https://github.com/kestra-io/kestra/security/advisories/GHSA-r56g-q4p6-m3p6	poc	yes	partial
CVE-2026-73608	8,6	SiYuan's development branch (endpoint introduced by commit; v3	Missing Authorization	prior to 3.7.4	https://github.com/siyuan-note/siyuan/security/advisories/GHSA-9cgf-hhrg-7v45 https://www.vulncheck.com/advisories/siyuan-before-authorization-bypass-via-getattributeviewsearchtarget	poc	yes	partial
CVE-2026-19228	8,5	GitLab EE affecting all	Authorization Bypass Through User-Controlled Key	19; before 19.1.4 and 19.2; before 19.2.2	https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-2-released/ https://gitlab.com/gitlab-org/gitlab/-/work_items/603347	none	no	partial
CVE-2026-18634	8,4	the one of the service of GMS application	Deserialization of Untrusted Data	9.5; 9510.1044) and earlier	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0011	none	no	total
CVE-2026-19557	8,3	TabStrip in Google Chrome on Mac	Use After Free	prior to 151.0.7922.137	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01815628406.html https://issues.chromium.org/issues/534867485	none	no	total
CVE-2026-66154	8,3	a GMS application	Improper Certificate Validation	9.5; 9510.1044) and earlier	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0011	none	no	total
CVE-2026-14679	8,2	PostgreSQL argument name matching	Stack-based Buffer Overflow	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-14679/	none	no	partial
CVE-2026-73650	8,2	SVGO, short for SVG Optimizer	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'); Incomplete List of Disallowed Inputs	in versions 1 through 3	https://github.com/svg/svgo/commit/628e3bc7336625a30365d0a9b60185307d852466 https://github.com/svg/svgo/commit/72a23886b4698b27624b936f3a15a80afd36d75f https://github.com/svg/svgo/commit/f529cfccc6c154d6f6eabe276ec637a8c5db6763 https://github.com/svg/svgo/releases/tag/v2.8.3 https://github.com/svg/svgo/releases/tag/v3.3.4 https://github.com/svg/svgo/releases/tag/v4.0.2			
CVE-2026-14668	8,1	Type confusion regarding input of PostgreSQL ctid data type selectivity estimator	Access of Resource Using Incompatible Type ('Type Confusion')	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-14668/	none	no	partial
CVE-2026-6464	8,1	PostgreSQL psql COPY	Inclusion of Functionality from Untrusted Control Sphere	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-6464/	none	no	total
CVE-2026-70465	8,1	Fortinet FortiClientWindows	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7.4.0 through 7.4.3; 7.2.0 through 7.2.11	https://fortiguard.fortinet.com/psirt/FG-IR-26-156	none	no	total
CVE-2026-70468	8,1	Fortinet FortiManager	Authentication Bypass Using an Alternate Path or Channel	7.4.3 through 7.4.5; 7.2.5 through 7.2.9	https://fortiguard.fortinet.com/psirt/FG-IR-26-160	none	no	total
CVE-2026-72665	8,1	Kibana	Missing Authorization	8.5.0 through 8.19.19; 9.0.0 through 9.4.4	https://discuss.elastic.co/t/kibana-8-19-20-and-9-4-5-security-update-esa-2026-96/389528			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-73515	8,1	PostGIS	Out-of-bounds Read	before 3.7.0beta2	https://gitea.osgeo.org/postgis/postgis/raw/tag/3.7.0beta2/NEWS https://mehmetince.net/part-1-6-systemic-risks-in-the-managed-postgresql-industry-extension-risks-are-real-exploiting-postgis-memory-corruption-bug-at-neondb-supabase-and-many-more/ https://www.vulncheck.com/advisories/postgis-0beta2-out-of-bounds-read-via-flatgeobuf-buffer	poc	no	total
CVE-2026-12234	7,8	subsys/net/lib/sockets/sockets	Time-of-check Time-of-use (TOCTOU) Race Condition	2.3.0 prior to 4.4.2	https://github.com/zephyrproject-rtos/zephyr/commit/2e0f9cf05be61056ed1a94dab51b832fbad27e2c https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-fcp3-vrr2-xfjv	poc	no	total
CVE-2026-14478	7,8	A maliciously created executable, when executed on the victim's machine, may	Incorrect Permission Assignment for Critical Resource	2.22.0 prior to 2.23.0	https://emsfs.autodesk.com/utility/odis/1/installer/latest/AdODIS-installer.exe https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0013	none	no	total
CVE-2026-63423	7,8	Lenovo Accessories and Display Manager for Enterprise for Windows that	Use of Hard-coded Cryptographic Key	prior to 1.0.9	https://support.lenovo.com/us/en/downloads/ds568567 https://support.lenovo.com/us/en/product_security/LEN-213038	none	no	total
CVE-2026-63425	7,8	Lenovo Dock Manager that could allow a local authenticated user to execute arbitrary code with elevated privileges	Incorrect Default Permissions	prior to 1.6.5.3	https://support.lenovo.com/us/en/product_security/LEN-223470 https://support.lenovo.com/us/en/solutions/ht037099#dm	none	no	total
CVE-2026-66149	7,8	the SonicWall Email Security appliance	Improper Control of Generation of Code ('Code Injection')	10.0.35.8405 and earlier versions	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0012	none	no	total
CVE-2026-73325	7,8	Fujitsu Research's OneCompression library	Deserialization of Untrusted Data	1.2.0 and earlier	https://pypi.org/project/onecomp/ https://pypi.org/project/onecomp/1.2.1/ https://www.vulncheck.com/advisories/fujitsu-onecompression-arbitrary-code-execution-via-torch-load-deserialization	none	no	total
CVE-2026-73505	7,8	Oh My Posh	Improper Control of Generation of Code ('Code Injection'); Improper Neutralization of Special Elements Used in a Template Engine	Prior to 29.35.1	https://github.com/JanDeDobbeleer/oh-my-posh/commit/88ddbe0b0a4dd13cc345996108c9869493f2c690 https://github.com/JanDeDobbeleer/oh-my-posh/pull/7711 https://github.com/JanDeDobbeleer/oh-my-posh/releases/tag/v29.35.1 https://github.com/JanDeDobbeleer/oh-my-posh/security/advisories/GHSA-6xj8-gv9j-xcjg	poc	no	total
CVE-2026-65582	7,7	AI Hub	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	<= 1.3.10	https://patchstack.com/database/wordpress/theme/aihub/vulnerability/wordpress-ai-hub-theme-1-3-10-arbitrary-file-download-vulnerability?_s_id=cve	none	no	partial
CVE-2026-66661	7,7	Directories Pro	Incorrect Privilege Assignment	<= 2.0.5	https://patchstack.com/database/wordpress/plugin/directories-pro/vulnerability/wordpress-directories-pro-plugin-2-0-5-privilege-escalation-vulnerability?_s_id=cve	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-2026-73498	7,7	MCP Atlassian	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to 0.22.0	https://github.com/sooperset/mcp-atlassian/commit/b041733473f95119dd539542a43c280737a8e460 https://github.com/sooperset/mcp-atlassian/pull/1448 https://github.com/sooperset/mcp-atlassian/releases/tag/v0.22.0 https://github.com/sooperset/mcp-atlassian/security/advisories/GHSA-q5r6-qv6m-f5jv	poc	no	partial
CVE-2026-73530	7,7	Flyto2 Core	Server-Side Request Forgery (SSRF)	before 2.28.0	https://github.com/flytohub/flyto-core/releases/tag/v2.28.0 https://github.com/flytohub/flyto-core/security/advisories/GHSA-gc4h-hj7x-gp5p https://www.vulncheck.com/advisories/flyto2-core-ssrf-guard-bypass-via-is-private-ip	poc	no	partial
CVE-2026-73346	7,6	MailChimp For WooCommerce	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	< 6.2	https://patchstack.com/database/wordpress/plugin/mailchimp-for-woocommerce/vulnerability/wordpress-mailchimp-for-woocommerce-plugin-6-2-sql-injection-vulnerability?_s_id=cve	none	no	partial
CVE-2026-73509	7,6	OpenList a file list program that	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to 4.2.4	https://github.com/OpenListTeam/OpenList/commit/651da18da4c647d96648d4bb64462baac1c37e04 https://github.com/OpenListTeam/OpenList/releases/tag/v4.2.4 https://github.com/OpenListTeam/OpenList/security/advisories/GHSA-95cv-r8x4-vh75	poc	no	partial
CVE-2019-25765	7,5	ASP-CMS; the commentList	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://github.com/projectdiscovery/nuclei-templates/issues/7968 https://web.archive.org/web/20201001011935/https://www.safeinfo.me/2019/07/22/aspcms-lou-dong-ji-he.html https://web.archive.org/web/20220425041152/https://asp-cms.sourceforge.net/ https://www.ddpoc.com/DVB-2021-821.html https://www.vulncheck.com/advisories/asp-cms-sql-injection-via-commentlist-asp-id-parameter			
CVE-2024-58374	7,5	Hongjing e-HR; the getSdutyTree servlet endpoint that	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://cn-sec.com/archives/2926383.html https://www.ddpoc.com/DVB-2024-7391.html https://www.vulncheck.com/advisories/hongjing-e-hr-unauthenticated-sql-injection-via-getsdutytree	poc	yes	partial
CVE-2026-14456	7,5	Issue summary: When an OpenSSL QUIC server (Listener SSL object)	Allocation of Resources Without Limits or Throttling	4.0.0 prior to 4.0.2; 3.6.0 prior to 3.6.4; 3.5.0 prior to 3.5.8	https://github.com/openssl/openssl/commit/08e7756c3900bcfd77a720e7b74e27d6e4ed01a9 https://github.com/openssl/openssl/commit/4084152e040329ca0194c4c1750b9b46d00a5b6b https://github.com/openssl/openssl/commit/f2f1465f2d2e5c61dfeac4d20fd093797d821139 https://openssl-library.org/news/secadv/20260813.txt http://www.openwall.com/lists/oss-security/2026/08/13/4	none	yes	partial
CVE-2026-14925	7,5	The Import WP WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 2.14.23	https://wpscan.com/vulnerability/67be2cc3-06d3-419e-8ca4-6dad442a02ca/	poc	yes	partial
CVE-2026-16253	7,5	The Total Upkeep WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 1.17.3	https://wpscan.com/vulnerability/97abf25a-48d4-4dfa-a7a3-de88455be7eb/	poc	yes	partial
CVE-2026-18048	7,5	The WP Photo Album Plus WordPress plugin	External Control of File Name or Path	before 9.2.07.002	https://wpscan.com/vulnerability/fbc145d3-a582-4975-bc6b-e56e633e51e6/	poc	yes	partial
CVE-2026-18789	7,5	The Ezoic WordPress plugin	Missing Authorization	before 2.23.1	https://wpscan.com/vulnerability/1e2ce237-dc91-4144-875a-339b5ea05f3a/	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-2026-19481	7,5	@fastify/busboy	Improper Check for Unusual or Exceptional Conditions	In versions 1.0.0 through 3.2.0	https://cna.openjsf.org/security-advisories.html https://github.com/fastify/busboy/security/advisories/GHSA-x8mw-p69m-v3mx	none	yes	partial
CVE-2026-19558	7,5	Extensions in Google Chrome	Use After Free	prior to 151.0.7922.137	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01815628406.html https://issues.chromium.org/issues/536676756	none	no	total
CVE-2026-47717	7,5	FUXA	Insertion of Sensitive Information Into Sent Data	= 1.3.0	https://github.com/frangoteam/FUXA/releases/tag/v1.3.1 https://github.com/frangoteam/FUXA/security/advisories/GHSA-g3w6-g3hc-c5x6	poc	yes	partial
CVE-2026-61980	7,5	OMGF Pro	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	<= 5.2.7	https://patchstack.com/database/wordpress/plugin/host-google-fonts-pro/vulnerability/wordpress-omgf-pro-plugin-5-2-7-arbitrary-file-download-vulnerability?_s_id=cve	none	yes	partial
CVE-2026-65370	7,5	servicetalk	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	prior to 0.42.65	https://github.com/apple/servicetalk/security/advisories/GHSA-56h2-h3h4-m9x6	none	yes	partial
CVE-2026-67991	7,5	crmne/ruby_llm at commit fa6f279847d6d7027814539d9c0dfc3bbdfd2a83	Inefficient Regular Expression Complexity		https://gist.github.com/Zykis1024/9f2d68fa3fd4e3a0ab83063bbe61a8e2 https://github.com/crmne/ruby_llm https://github.com/crmne/ruby_llm/blob/fa6f279847d6d7027814539d9c0dfc3bbdfd2a83/lib/ruby_llm/utils.rb#L13	none	yes	partial
CVE-2026-73188	7,5	KiviCare	Authentication Bypass Using an Alternate Path or Channel	<= 4.5.1	https://patchstack.com/database/wordpress/plugin/kivicare-clinic-management-system/vulnerability/wordpress-kivicare-plugin-4-5-1-sensitive-data-exposure-vulnerability?_s_id=cve	none	yes	partial
CVE-2026-73507	7,5	Netty	Uncontrolled Resource Consumption	Prior to 4.1.136.Final and 4.2.16.Final	https://github.com/netty/netty/commit/5b68c61f37aa4a3045cba624cbea239655c9003b https://github.com/netty/netty/commit/bb2ff68a1fb71cb4b0eb9a9e17b66c52aff680c6 https://github.com/netty/netty/releases/tag/netty-4.1.136.Final https://github.com/netty/netty/releases/tag/netty-4.2.16.Final https://github.com/netty/netty/security/advisories/GHSA-v74w-7mr3-4qg3			
CVE-2026-73561	7,5	Hub	Uncontrolled Resource Consumption	Prior to 0.2.16	https://github.com/anephenix/hub/commit/931576db3cdbf4f1583bd2c3c8759c4f4e032ab3 https://github.com/anephenix/hub/security/advisories/GHSA-g5vv-q72c-7j78 https://github.com/anephenix/hub/tree/v0.2.16			
CVE-2026-73566	7,5	node-tar	Uncontrolled Resource Consumption; Uncontrolled Recursion	Prior to 7.5.21	https://github.com/isaacs/node-tar/commit/631ae59121bf8fc8a22bbae35f074cb9b789cd4a https://github.com/isaacs/node-tar/security/advisories/GHSA-r292-9mhp-454m			
CVE-2026-73568	7,5	py-libp2p	Uncontrolled Resource Consumption	0.7.0 and earlier	https://github.com/libp2p/py-libp2p/commit/146ea87d1a20cc7dacf684ecf7c204543be04b37 https://github.com/libp2p/py-libp2p/security/advisories/GHSA-hmj8-5xmh-5573	poc	yes	partial
CVE-2026-73643	7,5	js-yaml	Inefficient Algorithmic Complexity	>= 5.0.0, < 5.2.2	https://github.com/nodeca/js-yaml/commit/3e5240f9cbe645ce5afb58524954a13c8539c853 https://github.com/nodeca/js-yaml/security/advisories/GHSA-pm4m-ph32-ghv5			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-49857	7,4	auth-fetch-mcp	Server-Side Request Forgery (SSRF)	< 3.0.2	https://github.com/vmw0407/auth-fetch-mcp/commit/c5c523cd55b24ae1680c5bacef95d59a81ae3450 https://github.com/vmw0407/auth-fetch-mcp/releases/tag/v3.0.1 https://github.com/vmw0407/auth-fetch-mcp/security/advisories/GHSA-pvrj-8cg3-j5f8	none	no	partial
CVE-2026-19757	7,3	Dromara lamp-cloud	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to 5.10.0.	https://github.com/dromara/lamp-cloud/ https://github.com/dromara/lamp-cloud/issues/412 https://vuldb.com/cve/CVE-2026-19757 https://vuldb.com/submit/868961 https://vuldb.com/vuln/389602 https://vuldb.com/vuln/389602/cti			
CVE-2026-19762	7,3	DTStack Taier	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1.4.0	https://github.com/DTStack/Taier/ https://github.com/DTStack/Taier/issues/1203 https://vuldb.com/cve/CVE-2026-19762 https://vuldb.com/submit/868966 https://vuldb.com/vuln/389665 https://vuldb.com/vuln/389665/cti			
CVE-2026-18109	7,2	The W3 Total Cache plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.10.3	https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.2/UserExperience_LazyLoad_Mutator.php#L162 https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.2/UserExperience_LazyLoad_Mutator.php#L403 https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.2/UserExperience_LazyLoad_Mutator.php#L85 https://plugins.trac.wordpress.org/browser/w3-total-cache/tags/2.10.2/UserExperience_LazyLoad_Plugin.php#L116 https://plugins.trac.wordpress.org/changeset/3635675/w3-total-cache/trunk/UserExperience_LazyLoad_Mutator.php https://plugins.trac.wordpress.org/changeset?old_path=%2Fw3-total-cache/tags/2.10.3&new_path=%2Fw3-total-cache/tags/2.10.4			
CVE-2026-18146	7,2	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 6.2.11	https://plugins.trac.wordpress.org/browser/fluentform/tags/6.2.8/app/Services/FormBuilder/Notifications/EmailNotification.php#L196 https://plugins.trac.wordpress.org/browser/fluentform/tags/6.2.8/app/Services/FormBuilder/ShortCodeParser.php#L142 https://plugins.trac.wordpress.org/browser/fluentform/tags/6.2.8/app/Services/FormBuilder/ShortCodeParser.php#L145 https://plugins.trac.wordpress.org/browser/fluentform/tags/6.2.8/assets/js/form_entries.js#L2 https://plugins.trac.wordpress.org/browser/fluentform/tags/6.2.8/boot/globals.php#L98 https://plugins.trac.wordpress.org/changeset/3640683/fluentform/trunk/app/Services/FormBuilder/ShortCodeParser.php	none	yes	partial
CVE-2026-6471	7,2	PostgreSQL logical decoding	Missing Authorization	18 prior to 18.5; 17 prior to 17.11; 16 prior to 16.15; 15 prior to 15.19; prior to 14.24	https://www.postgresql.org/support/security/CVE-2026-6471/	none	no	total
CVE-2026-16294	7,1	The PowerPress Podcasting plugin by Blubrry WordPress plugin	Server-Side Request Forgery (SSRF)	before 11.17.1	https://wpscan.com/vulnerability/9363aaff-40d6-41c0-8edd-cbf671240ad2/	poc	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-2026-28154	7,1	snstheme Samex - Clean, Minimal Shop WooCommerce WordPress Theme and sns-theme M	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	through 2.5; through 1.7.	https://patchstack.com/database/wordpress/theme/manh/vulnerability/wordpress-m-anh-theme-1-7-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve https://patchstack.com/database/wordpress/theme/samex/vulnerability/wordpress-samex-clean-minimal-shop-woocommerce-wordpress-theme-theme-2-5-cross-site-scripting-xss-vulnerability?_s_id=cve			
CVE-2026-72630	7,1	Kibana Fleet	Incorrect Authorization	8.19.0 through 8.19.19; 9.0.0 through 9.4.4; 9.5.0	https://discuss.elastic.co/t/kibana-8-19-20-9-4-5-9-5-1-security-update-esa-2026-127/389531	none	no	total

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
-	-	-

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
Privacy Policy	https://cybersecuritynews.com/privacy-policy-2
10 Best Secure Web Gateway Vendors In 2026	https://cybersecuritynews.com/best-secure-web-gateway
New DRAM Scrambling Attack Exposes CPU's Most Protected Memory Zones	https://cybersecuritynews.com/dram-scrambling-attack
Apple Urges Mercenary Spyware Targets to Enable Lockdown Mode Immediately	https://cybersecuritynews.com/apple-sends-spyware-attack-alerts
Apple sends new 'Threat Notification' alerts over mercenary spyware attacks	https://bleepingcomputer.com/news/apple/apple-sends-new-threat-notification-alerts-over-mercenary-spyware-attacks
Ukraine shuts down 94 fraudulent call centers, seize millions in cash	https://bleepingcomputer.com/news/security/ukraine-shuts-down-94-fraudulent-call-centers-seize-millions-in-cash

Akira hackers disable EDR with Safe Mode, steal data but fail to encrypt	https://bleepingcomputer.com/news/security/akira-hackers-disable-edr-with-safe-mode-steal-data-but-fail-to-encrypt
Hackers breach govt webmail while running parallel crypto fraud	https://bleepingcomputer.com/news/security/hackers-breach-govt-webmail-while-running-parallel-crypto-fraud
AI 'watermark removers' flood the web. Almost none can prove they work.	https://bleepingcomputer.com/news/security/ai-watermark-removers-flood-the-web-almost-none-can-prove-they-work
Beacon CRM Confirms Full Database Theft After AWS Access Key Breach	https://cybersecuritynews.com/beacon-crm-database-theft
Google Targets 2027 for First Major Post-Quantum Security Milestone	https://infosecurity-magazine.com/news/google-cloud-post-quantum-roadmap
Cybersecurity M&A Roundup: 21 Deals Announced in July 2026	https://securityweek.com/cybersecurity-ma-roundup-21-deals-announced-in-july-2026
AmnesiaStealer Hijacks Chromium Sessions to Give Attackers Live Browser Control on macOS	https://thehackernews.com/2026/08/amnesiastealer-hijacks-chromium.html
White House taps security firms for offensive hack-back operations	https://bleepingcomputer.com/news/security/white-house-taps-security-firms-for-offensive-hack-back-operations
North Korean IT Workers Use AI-Forged IDs and Remote Desktops to Become Trusted Employees	https://cybersecuritynews.com/north-korean-it-workers-ai-forged-ids
Trump Authorizes Private Sector Participation in Offensive Cyber Opera	https://infosecurity-magazine.com/news/trump-private-offensive-cyber
WhatsApp rolls out new feature that flags potential scam messages	https://bleepingcomputer.com/news/security/whatsapp-rolls-out-new-feature-that-flags-potential-scam-messages
Venture Firm Team8 Secures Additional $365 Million	https://securityweek.com/venture-firm-team8-secures-additional-365-million
White House Mobilizes Security Firms for Operations Against Foreign Cybercrime Gangs	https://securityweek.com/white-house-mobilizes-security-firms-for-operations-against-foreign-cybercrime-gangs
ICO Reprimands Criminal Records Office After 2023 Breach	https://infosecurity-magazine.com/news/ico-reprimands-acro-records-office

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
Exposed AWS Access Key Linked to Data Breach Affecting 1500+ UK Charit	https://infosecurity-magazine.com/news/exposed-aws-key-data-charities
Trezor discloses data breach affecting nearly 14,000 customers	https://bleepingcomputer.com/news/security/trezor-discloses-data-breach-affecting-nearly-14-000-customers
Trezor ShipMonk Data Breach Exposes Personal Data of Over 13,000 Hardware Wallet Customers	https://cybersecuritynews.com/trezor-shipmonk-data-breach

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
Global Threat Campaign Hits Critical VMware vCenter Flaw	https://darkreading.com/vulnerabilities-threats/global-threat-campaign-critical-vmware-vcenter-flaw
ThreatsDay: GhostJacking AI Attacks, EtherHiding ClickFix, Cursor CLI Flaw + 17 More Stories	https://thehackernews.com/2026/08/threatsday-ghostjacking-ai-attacks.html
Critical VMware vCenter RCE flaw exploited for reverse SSH access	https://bleepingcomputer.com/news/security/critical-vmware-vcenter-rce-flaw-exploited-for-reverse-ssh-access
Adobe Commerce Bug Targeted Immediately After Disclosure	https://securityweek.com/adobe-commerce-bug-targeted-immediately-after-disclosure
Microsoft Exchange Server Vulnerabilities Enable DoS, Privilege Escalation, and RCE Attacks	https://cybersecuritynews.com/microsoft-exchange-server-vulnerabilities-rce
vCenter Flaw Exploited Just Five Days After Disclosure	https://infosecurity-magazine.com/news/vcenter-cve-2026-59310-exploited
CISA Warns of Windows Ancillary Function 0-Day Vulnerability Exploited in Attacks	https://cybersecuritynews.com/windows-ancillary-function-0-day-exploited
Critical VMware vCenter Vulnerability in Attackers' Crosshairs	https://securityweek.com/critical-vmware-vcenter-vulnerability-in-attackers-crosshairs
Nightmare Eclipse Drops Windows Zero-Day Exploit 'ShieldBreak'	https://securityweek.com/nightmare-eclipse-drops-windows-zero-day-exploit-shieldbreak
Belgium's eID Authentication Opens Citizen Accounts to RCE	https://darkreading.com/application-security/belgium-eid-authentication-citizen-accounts-rce
Attackers Exploit SharePoint Authentication Bypass After Public PoC Release	https://thehackernews.com/2026/08/attackers-exploit-sharepoint.html
Cisco Firewall 0-Day Vulnerability Exploited in the Wild to Trigger DoS Condition	https://cybersecuritynews.com/cisco-firewall-0-day-vulnerability
Critical WordPress RCE Vulnerability Allows Authors to Execute Code via Malicious PNG File	https://cybersecuritynews.com/wordpress-imagick-rce-vulnerability
Hackers exploit critical Adobe Commerce flaw to hijack customer accounts	https://bleepingcomputer.com/news/security/hackers-exploit-critical-adobe-commerce-flaw-to-hijack-customer-accounts
Lazarus hackers exploited Windows zero-day to target defense firms	https://bleepingcomputer.com/news/security/lazarus-hackers-exploited-windows-zero-day-to-target-defense-firms
SharePoint Vulnerability Exploited Shortly After PoC Release	https://securityweek.com/sharepoint-vulnerability-exploited-shortly-after-poc-release
Lazarus Used Post-Quantum Key Exchange to Deliver Zero-Day	https://infosecurity-magazine.com/news/lazarus-post-quantum-key-dream-job
OpenAI, Anthropic, Google API Flaw Let Weaker AI Models Decode Stronger Models' Reasoning	https://thehackernews.com/2026/08/openai-anthropic-google-api-flaw-let.html
Chipmaker Patch Tuesday: Intel, AMD Fix Over 80 Vulnerabilities Combined	https://securityweek.com/chipmaker-patch-tuesday-intel-amd-fix-over-80-vulnerabilities-combined
New Microsoft Defender 'ShieldBreak' zero-day grants SYSTEM privileges	https://bleepingcomputer.com/news/security/new-microsoft-defender-shieldbreak-zero-day-grants-system-privileges

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
Unpatched GeoServer Zero-Day Targeted in Active Exploitation Attempts, Can Lead to RCE	https://thehackernews.com/2026/08/unpatched-geoserver-zero-day-targeted.html
Microsoft patches LegacyHive Windows zero-day vulnerability	https://bleepingcomputer.com/news/microsoft/microsoft-patches-legacyhive-windows-zero-day-vulnerability
Fortinet Patches Multiple Authentication Vulnerabilities in FortiWeb, FortiManager, and FortiClient	https://cybersecuritynews.com/fortinet-authentication-vulnerabilities
GitLab 19.2.2 Patches 13 Security Flaws, Including High-Severity XSS and CI/CD Authorization Flaws	https://cybersecuritynews.com/gitlab-patches-13-security-flaws
WordPress 7.0.4 Patches Remote Code Execution Vulnerability	https://securityweek.com/wordpress-7-0-4-patches-remote-code-execution-vulnerability
Fortinet Patches Authentication Flaws in FortiWeb and FortiManager	https://securityweek.com/fortinet-patches-authentication-flaws-in-fortiweb-and-fortimanager
Palo Alto Networks Patches 11 New Vulnerabilities Across PAN-OS, GlobalProtect, and Prisma Access	https://cybersecuritynews.com/palo-alto-networks-vulnerabilities
Adobe Patches Three CVSS 10.0 ColdFusion and Campaign Classic Flaws	https://thehackernews.com/2026/08/adobe-patches-three-cvss-100-coldfusion.html
Ivanti EPM Update Patches Remotely Exploitable Flaws	https://securityweek.com/ivanti-epm-update-patches-remotely-exploitable-flaws
Microsoft Fixes 400 Flaws on August Patch Tuesday	https://infosecurity-magazine.com/news/microsoft-fixes-400-flaws-august
SonicWall Patches Critical Vulnerabilities in Discontinued GMS Platform	https://securityweek.com/sonicwall-patches-critical-vulnerabilities-in-discontinued-gms-platform
Cisco Patches Firewall Zero-Day Exploited for DoS Attacks	https://securityweek.com/cisco-patches-firewall-zero-day-exploited-for-dos-attacks

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
AmnesiaStealer macOS Malware Hijacks Browser Sessions via Fake GitHub Lure	https://cybersecuritynews.com/amnesiastealer-macos-malware
'Jewelbug' APT Balances State Espionage & Cryptocurrency Theft	https://darkreading.com/threat-intelligence/jewelbug-apt-state-espionage-cryptocurrency-theft
Akira Affiliate Crashes Ransomware After Attempting EDR Evasion	https://infosecurity-magazine.com/news/akira-affiliate-crashes-ransomware

Android malware combo takes out loans and relays victims' credit cards	https://bleepingcomputer.com/news/security/android-malware-combo-takes-out-loans-and-relays-victims-credit-cards
Long-running Data Theft Campaign Targets Salesforce, ServiceNow	https://darkreading.com/cyberattacks-data-breaches/long-running-data-theft-campaign-salesforce-servicenow
Lazarus Exploits Windows Zero-Day to Gain SYSTEM Access and Deploy Backdoor	https://thehackernews.com/2026/08/lazarus-exploits-windows-zero-day-to.html
Eclipse Ransomware Launches RaaS Platform Targeting Windows, Linux, and ESXi Infrastructure	https://cybersecuritynews.com/eclipse-ransomware-raas-platform
WindRelay Malware Pairs With SpyNote RAT in Live-Call Scam	https://infosecurity-magazine.com/news/windrelay-nfc-relay-spynote-rat
Gunra Ransomware Exploits Fortinet Flaws to Target Critical Infrastruc	https://infosecurity-magazine.com/news/gunra-ransomware-fortinet-flaws
Windows AFD.sys 0-Day Actively Exploited by Lazarus Hackers to Deploy FudModule Rootkit	https://cybersecuritynews.com/windows-afd-sys-zero-day-exploited
Gunra Ransomware Gang Exploits Fortinet Flaws, Bypasses MFA	https://darkreading.com/cyberattacks-data-breaches/gunra-ransomware-gang-fortinet-flaws-bypasses-mfa

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 Microsegmentation Tools in 2026	https://cybersecuritynews.com/best-microsegmentation-tools
Blacklight Toolkit Finds Codex, Claude Code, and Cursor Artifacts Exposing Tokens and Session Data	https://cybersecuritynews.com/blacklight-toolkit

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 12/08/2026–14/08/2026 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/