

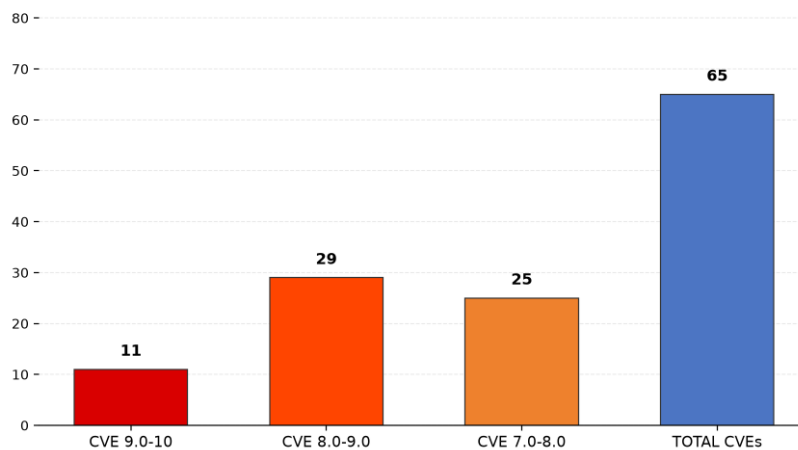


Newsletter on system vulnerabilities and cybersecurity news.

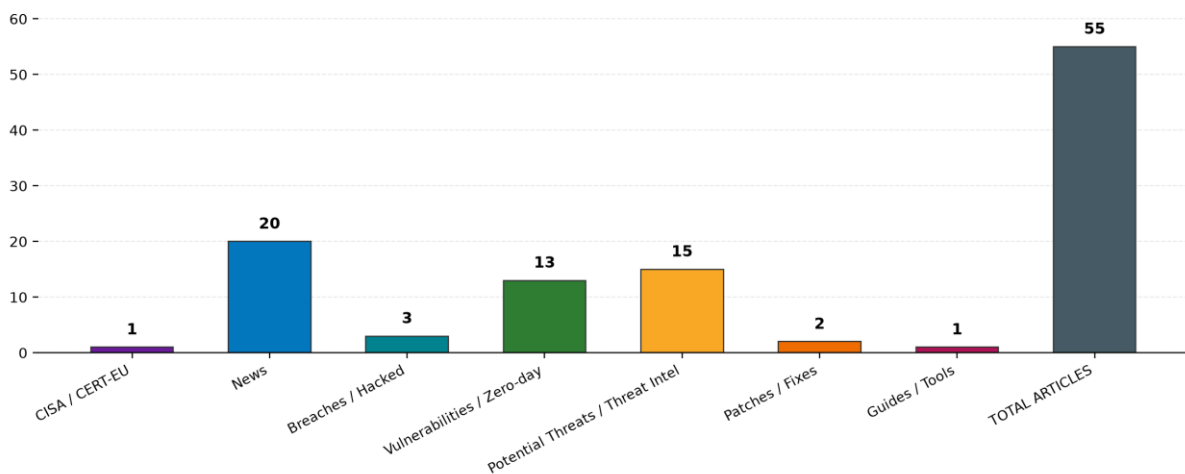
National Cyber Security Authority (NCSA)

Date: 19/09/2026 - 22/09/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories.....	11
News.....	12
Breaches / Compromised / Hacked.....	13
Vulnerabilities / Flaws / Zero-day.....	13
Patches / Updates / Fixes	14
Potential threats / Threat intelligence	14
Guides / Tools.....	15
References.....	16
Annex – Websites with vendor specific vulnerabilities	17

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-2026-94493	10,0	Gigatech PDV5701	Improper Authentication; Missing Authentication for Critical Function	1.0.31_240305_112640	https://github.com/CSDV/cve/issues/2 https://vuldb.com/cve/CVE-2026-94493 https://vuldb.com/submit/895425 https://vuldb.com/vuln/408193 https://vuldb.com/vuln/408193/ctj			
CVE-2026-79920	9,9	Ajenti	Missing Authorization	Prior to version 2.2.16	https://github.com/ajenti/ajenti/commit/3a8cbee32df4c5033796f19af4210011163a6f6e https://github.com/ajenti/ajenti/commit/f07f02e0cdeeb3e528c1d5af28e27fd11623c49c https://github.com/ajenti/ajenti/releases/tag/v2.2.16 https://github.com/ajenti/ajenti/security/advisories/GHSA-A-8xf-5fw2-f99g	none	no	total
CVE-2026-93985	9,9	OpenPanel	Improper Control of Generation of Code ('Code Injection')	bad75bddc74d12d36cfb843f4531d3b830a8d994 and earlier	https://github.com/Openpanel-dev/openpanel/security/advisories/GHSA-6f7h-cvp6-w9w5 https://www.vulncheck.com/advisories/openpanel-js-runtime-javascript-template-sandbox-escape-rce	poc	no	total
CVE-2026-13355	9,8	The Meta Box AIO plugin for Word-Press	Improper Privilege Management	up to, and including, 3.11.0.; up to 4.5.6); up to 3.11.0)	https://metabox.io/changelog/ https://metabox.io/plugins/meta-box-aio/changelog/ https://www.wordfence.com/threat-intel/vulnerabilities/id/3b7b6e7e-b944-45f8-a6d8-bfd859bec0d1?source=cve			
CVE-2026-19658	9,8	The Give Tributes plugin for Word-Press	Deserialization of Untrusted Data	up to, and including, 2.3.1	https://www.liquidweb.com/software/qive/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0cdd5562-8755-4ca3-9c16-a5b364f8408b?source=cve			
CVE-2026-78030	9,8	DBI versions	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	versions before 1.653	https://github.com/perl5-dbi/dbi/commit/315c6ce703b8b3cbe9188062d9ec80730293554a.patch https://github.com/perl5-dbi/dbi/security/advisories/GHSA-wgmw-wqwx-3fr7 https://metacpan.org/release/HMBRAND/DBI-1.653/changes http://www.openwall.com/lists/oss-security/2026/09/19/4	none	yes	total
CVE-2026-85751	9,8	Mailu	Authentication Bypass by Spoofing; Reliance on Untrusted Inputs in a Security Decision	>= 2.0.0, < 2024.06.55; < 2.7.3	https://github.com/Mailu/Mailu/commit/dffa97cbd889ab208246372ce9c86e99abb27ae9 https://github.com/Mailu/Mailu/commit/ff4003d045753013470945336448dbd790cac778 https://github.com/Mailu/Mailu/pull/4070 https://github.com/Mailu/Mailu/pull/4071 https://github.com/Mailu/Mailu/releases/tag/2024.06.55 https://github.com/Mailu/Mailu/security/advisories/GHSA-rfjh-4wcq-74xq	none	yes	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-90817	9,8	the survey passthrough routing and Data Import processing logic, in which a malicious user; REDCap	External Control of File Name or Path; Improper Control of Generation of Code ('Code Injection')	13.3.0	https://www.securifera.com/advisories/	none	yes	total
CVE-2026-94083	9,4	Suricata	Access of Resource Using Incompatible Type ('Type Confusion')	before 8.0.7	https://forum.suricata.io/t/suricata-8-0-7-released/6467 https://github.com/OISF/suricata/commit/e574009add9c208f319e1d9d15b3bb1229c88074 https://github.com/OISF/suricata/compare/suricata-8.0.6...suricata-8.0.7			
CVE-2026-58491	9,3	Warpgate	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 0.25.5	https://github.com/warptech/warpgate/commit/eab0548f018d95b5f96f8e913527000e05ed93a2 https://github.com/warptech/warpgate/releases/tag/v0.25.5 https://github.com/warptech/warpgate/security/advisories/GHSA-3c3w-75j2-7h74			
CVE-2026-75885	9,3	the OpenShift console	Server-Side Request Forgery (SSRF)		https://access.redhat.com/security/cve/CVE-2026-75885 https://bugzilla.redhat.com/show_bug.cgi?id=2517885	none	yes	partial
CVE-2026-53940	8,8	Conda	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); External Control of File Name or Path	Prior to 26.5.2	https://github.com/conda/conda/commit/3987c86ccd5527177e96b48bd4dc177dd2c9baa https://github.com/conda/conda/pull/16168 https://github.com/conda/conda/releases/tag/26.5.2 https://github.com/conda/conda/security/advisories/GHSA-9m8m-c4i3-ri2c	poc	no	total
CVE-2026-55159	8,8	luci-app-adblock-fast	Improper Neutralization of CRLF Sequences ('CRLF Injection')	Prior to 1.2.4-2	https://github.com/openwrt/luci/commit/9ccd99b5898457e5ef39dc21aea226d7fb6e5c7e https://github.com/openwrt/luci/commit/f67461fd0255bf992b2b559c22ec288067f2f9da https://github.com/openwrt/luci/pull/8705 https://github.com/openwrt/luci/security/advisories/GHSA-qgpf-xrph-wq5v			
CVE-2026-55897	8,8	luci-app-advanced-reboot	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 1.1.2-6	https://github.com/openwrt/luci/commit/2df00deb122093cbf429266ffef7ad06aaecb48f https://github.com/openwrt/luci/commit/f85102548ee8325bfd581a0327b210b5f7670829 https://github.com/openwrt/luci/pull/8710 https://github.com/openwrt/luci/security/advisories/GHSA-vi96-f37q-37f6	poc	no	total
CVE-2026-62182	8,8	KubeEdge	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	>= 1.21.0, < 1.21.2; >= 1.22.0, < 1.22.2; >= 1.23.0, < 1.23.1	https://github.com/kubeedge/kubeedge/blob/master/CHANGELOG/CHANGELOG-1.21.md https://github.com/kubeedge/kubeedge/blob/master/CHANGELOG/CHANGELOG-1.22.md https://github.com/kubeedge/kubeedge/blob/master/CHANGELOG/CHANGELOG-1.23.md https://github.com/kubeedge/kubeedge/commit/14f65fc6207787f266cbcb0dceac7f09a81bab2b https://github.com/kubeedge/kubeedge/commit/6309a335c8e5e3c154b6bb0a09292f5c7dc598dc https://github.com/kubeedge/kubeedge/commit/ee78415a36911c1a93e59a921c23b8e4ecd83e90			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-63116	8,8	deepstream	Missing Authorization	>= 10.1.0, < 10.1.1	https://github.com/deepstreamIO/deepstream.io/commit/1c2adde6581c53ef47e204364bc740bc3c2e2e2a https://github.com/deepstreamIO/deepstream.io/releases/tag/v10.1.1 https://github.com/deepstreamIO/deepstream.io/security/advisories/GHSA-89vx-jh4g-vq3w	poc	no	total
CVE-2026-82412	8,8	ntopng	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 6.7.260717	https://github.com/ntop/ntopng/commit/0d3156274f4d12db8b61432ebded10966c01f3e https://github.com/ntop/ntopng/commit/771b34a9d37f5de989eeca42f8f2e852db1c7e5e https://github.com/ntop/ntopng/commit/838ccd523a3d4a71b29a62f7653e572a1ffa5cf6 https://github.com/ntop/ntopng/commit/9f42a12251d881e3a20ebd667c1a2e6a6570c270 https://github.com/ntop/ntopng/security/advisories/GHSA-2c6p-4pfi-qv58	none	no	total
CVE-2026-86553	8,8	SmartLife	Improper Privilege Management	ZTE_SL_V2.8.2_ABRO AD and prior versions	https://support.zte.com.cn/zte-iccp-support-webui/bulletin/detail/2171542593031840100	none	no	total
CVE-2026-88409	8,8	FalkorDB (Redis module)		v4.20.1 to v4.20.4	https://github.com/FalkorDB/FalkorDB/issues/2399			
CVE-2026-92574	8,8	CRI-O checkpoint restore	Execution with Unnecessary Privileges	1.34 and later	https://access.redhat.com/security/cve/CVE-2026-92574 https://bugzilla.redhat.com/show_bug.cgi?id=2535436	none	no	total
CVE-2026-93993	8,8	Mistral Vibe	Inclusion of Functionality from Untrusted Control Sphere	before 2.25.5	https://github.com/mistralai/mistral-vibe https://github.com/mistralai/mistral-vibe/blob/19b5b74faa78d0816b8d4d4c7d7543fc3520678c/vibe/core/qitrepo.py#L411-L431 https://github.com/mistralai/mistral-vibe/commit/c069ffa1e12fb5f2487b489217c40ab97721d553 https://github.com/mistralai/mistral-vibe/issues/996 https://github.com/mistralai/mistral-vibe/releases/tag/v2.25.5 https://www.vulncheck.com/advisories/mistral-vibe-before-2.25.5-remote-code-execution-via-git-post-checkout	poc	no	total
CVE-2026-94104	8,8	NivoCart	Unrestricted Upload of File with Dangerous Type	through 2.4.0	https://github.com/nivocart/nivocart https://github.com/nivocart/nivocart/blob/6ea6600cda1263ae70c0aab0a70d31091a32c46b/upload/admin/controller/common/filemanager.php#L527-L562 https://github.com/nivocart/nivocart/blob/6ea6600cda1263ae70c0aab0a70d31091a32c46b/upload/admin/controller/common/filemanager_full.php https://github.com/nivocart/nivocart/issues/25 https://www.vulncheck.com/advisories/nivocart-through-2.4.0-arbitrary-file-upload-rce-via-filemanager			
CVE-2026-94106	8,8	getID3	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 1.9.26	https://github.com/JamesHeinrich/getID3 https://github.com/JamesHeinrich/getID3/blob/efffe762b02be155d0c32eeca57eff8a49bc4b5/getid3/write.vorbiscomment.php#L85-L110 https://github.com/JamesHeinrich/getID3/commit/2c6f3f96546f05746405872848114754ed7fe9b4 https://github.com/JamesHeinrich/getID3/commit/ce598c4f3823441d878c5a7a2a9f2f703a3e10b6 https://github.com/JamesHeinrich/getID3/issues/503 https://github.com/JamesHeinrich/getID3/releases/tag/v1.9.26	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-2026-94109	8,8	openEQUELLA	Improper Neutralization of Special Elements Used in a Template Engine	versions before 2026.1.0	https://github.com/openequella/openEQUELLA https://github.com/openequella/openEQUELLA/blob/8bd24b1dcf26cc3d74757e6b982fc1971a7d6767/Source/Plugins/Core/com.equella.core/src/com/tle/core/entity/service/impl/AbstractEntityServiceImpl.java#L230-L250 https://github.com/openequella/openEQUELLA/blob/8bd24b1dcf26cc3d74757e6b982fc1971a7d6767/Source/Plugins/Core/com.equella.core/src/com/tle/web/freemarker/BasicConfiguration.java https://github.com/openequella/openEQUELLA/blob/8bd24b1dcf26cc3d74757e6b982fc1971a7d6767/Source/Plugins/Core/com.equella.core/src/com/tle/web/portal/standard/renderer/FreemarkerPortletRenderer.java#L141-L170 https://github.com/openequella/openEQUELLA/commit/d6e165afc986f8a3ed912cdb367d5ad8c1eeab5c https://github.com/openequella/openEQUELLA/releases/tag/2026.1.0			
CVE-2026-94403	8,8	ColorFul iGameCenter	Untrusted Pointer Dereference	1.0.3.4	https://vuldb.com/cve/CVE-2026-94403 https://vuldb.com/submit/894821 https://vuldb.com/vuln/408110 https://vuldb.com/vuln/408110/ctj			
CVE-2026-94411	8,8	jshERP	Missing Authorization	3.6	https://github.com/LinYuanYi1/cve-request-poc/blob/master/jshERP/poc-01-userbusiness-self-privilege-escalation.py https://github.com/jishenghua/jshERP https://github.com/jishenghua/jshERP/blob/v3.6/jshERP-boot/src/main/java/com/jsh/erp/controller/UserBusinessController.java#L178-L198 https://www.vulncheck.com/advisories/jsherp-3.6-privilege-escalation-via-updateonevaluebykeyidandtype			
CVE-2026-94424	8,8	Moore Threads MTT S80 Driver Package	Improper Restriction of Operations within the Bounds of a Memory Buffer; Heap-based Buffer Overflow	up to 340.150.	https://vuldb.com/cve/CVE-2026-94424 https://vuldb.com/submit/894806 https://vuldb.com/vuln/408150 https://vuldb.com/vuln/408150/ctj			
CVE-2026-68928	8,6	Acode	Exposed Dangerous Method or Function; Missing Authorization; Improper Export of Android Application Components	>= 1.11.6, < 1.12.7	https://github.com/Acode-Foundation/Acode/commit/0a5237a3b140562dac877868137a784d6531894d https://github.com/Acode-Foundation/Acode/pull/2442 https://github.com/Acode-Foundation/Acode/releases/tag/v1.12.7 https://github.com/Acode-Foundation/Acode/security/advisories/GHSA-wm94-wp33-43qx	poc	no	total
CVE-2026-49811	8,4	Dell Command Monitor (DCM), versions	Incorrect Permission Assignment for Critical Resource	versions prior to 10.13.2	https://www.dell.com/support/kbdoc/en-us/000502473/dsa-2026-380-security-update-for-dell-command-monitor-dcm-for-an-incorrect-permission-assignment-for-critical-resource-vulnerability	none	no	total
CVE-2026-55071	8,4	MCP-for-Stata	Improper Control of Generation of Code ('Code Injection')	Prior to version 1.19.0	https://github.com/SepineTam/mcp-for-stata/releases/tag/v1.19.0 https://github.com/SepineTam/mcp-for-stata/security/advisories/GHSA-49m4-vp58-wqc9	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-2026-94488	8,2	Telegram Desktop	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 6.9.4	https://expatch.com/writeups/telegram-html-export-xss.html https://github.com/telegramdesktop/tdesktop/blob/v6.9.3/Telegram/SourceFiles/export/output/export_output.html.cpp https://github.com/telegramdesktop/tdesktop/commit/52c779bffa8dde3c5c09826add2607328fae0924 https://github.com/telegramdesktop/tdesktop/commit/8457d13aa795fadf99c955d2a04f00ebc3c59df9 https://github.com/telegramdesktop/tdesktop/releases/tag/v6.9.4 https://thehackernews.com/2026/09/telegram-desktop-flaw-lets-hidden.html	poc	no	total
CVE-2026-48826	8,1	HomeBox	Improper Privilege Management; Authorization Bypass Through User-Controlled Key	Prior to 0.26.0	https://github.com/sysadminsmedia/homebox/commit/e43216a80998df81d4418700696244144883160 https://github.com/sysadminsmedia/homebox/releases/tag/v0.26.0 https://github.com/sysadminsmedia/homebox/security/advisories/GHSA-559i-7w3w-4fr7	none	no	partial
CVE-2026-58269	8,1	Sync-in Server	Authentication Bypass Using an Alternate Path or Channel	Prior to version 2.4.0	https://github.com/Sync-in/server/security/advisories/GHSA-92cr-ixw4-5wjg			
CVE-2026-61628	8,1	nginx ignition	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	Prior to version 2.41.1	https://github.com/lucasdillmann/nginx-ignition/commit/0586b4e55ab780676d3553a2592979dfa2fb0183 https://github.com/lucasdillmann/nginx-ignition/security/advisories/GHSA-pxcx-fv34-x9p5	poc	no	total
CVE-2026-77560	8,1	Tinyauth	Improper Handling of Case Sensitivity; Not Failing Securely ('Failing Open'); Incorrect Authorization	Prior to 5.1.2	https://github.com/tinyauthapp/tinyauth/commit/80bc87188ec3aabc5104c249eaa7b997973b9275 https://github.com/tinyauthapp/tinyauth/commit/e75605b2c534ec83525a33603e16d76baca13399 https://github.com/tinyauthapp/tinyauth/pull/1000 https://github.com/tinyauthapp/tinyauth/pull/1028 https://github.com/tinyauthapp/tinyauth/releases/tag/v5.1.2 https://github.com/tinyauthapp/tinyauth/security/advisories/GHSA-328g-ix67-v94g	none	no	total
CVE-2026-80110	8,1	pki-core	Incorrect Authorization		https://access.redhat.com/security/cve/CVE-2026-80110 https://bugzilla.redhat.com/show_bug.cgi?id=2523749	none	no	total
CVE-2026-88097	8,1	Microsoft Edge (Chromium-based)	Use After Free	1.0.0.0 prior to 153.0.4234.46	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88097	none	no	total
CVE-2026-93992	8,1	Gopreed	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	through 2.0.0-beta.3	https://github.com/GopreedLab/gopreed https://github.com/GopreedLab/gopreed/blob/a5cd53f94c18ac65add684b1113fa5f0b47cc4da/pkg/download/extract.go#L284-L296 https://github.com/GopreedLab/gopreed/blob/a5cd53f94c18ac65add684b1113fa5f0b47cc4da/pkg/download/extract_7z.go#L45-L53 https://github.com/GopreedLab/gopreed/commit/38750d8505274e55cf11aa77f0694c71dd82f519 https://github.com/GopreedLab/gopreed/issues/1525 https://www.vulncheck.com/advisories/gopreed-through-2.0.0-beta.3-arbitrary-file-write-via-path-traversal	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-2026-94184	8,1	A stack-based buffer overflow flaw was found in fetchmail when built with NTLM; fetchmail when built with NTLM support	Stack-based Buffer Overflow	v5.0.8 through v6.6.6.	https://access.redhat.com/security/cve/CVE-2026-94184 https://bugzilla.redhat.com/show_bug.cgi?id=2537395 https://gitlab.com/fetchmail/fetchmail/-/commit/cb5be5c38471e0c19e519ace0bc569176317ea92 https://www.fetchmail.info/fetchmail-SA-2026-01.txt https://www.openwall.com/lists/oss-security/2026/06/27/8	none	no	total
CVE-2026-15801	8,0	CRI-O related to the container checkpoint and restore feature	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://access.redhat.com/security/cve/CVE-2026-15801 https://bugzilla.redhat.com/show_bug.cgi?id=2500823			
CVE-2026-17052	7,8	drivers/timeaware_gpio/timeaware_gpio_handlers	Out-of-bounds Write	3.5.0 prior to 4.4.2	https://github.com/zephyrproject-rtos/zephyr/commit/26264ff1c7c2174319394fa274af3f6f4dc221 https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-8qwg-x76h-8mpc	none	no	total
CVE-2026-49810	7,8	Dell Command Powershell Provider (DCPP), versions	Insertion of Sensitive Information into Log File	versions prior to 2.10.2	https://www.dell.com/support/kbdoc/en-us/000502472/dsa-2026-379-security-update-for-dell-command-powershell-provider-dcpp-for-a-credential-theft-via-powershell-event-log-vulnerability			
CVE-2026-55567	7,8	bleachbit	Time-of-check Time-of-use (TOCTOU) Race Condition	Prior to 6.0.1	https://github.com/bleachbit/bleachbit/commit/ee128238e92c7192f0c4d6406b1bd0cd9155e7e0 https://github.com/bleachbit/bleachbit/pull/1774 https://github.com/bleachbit/bleachbit/releases/tag/v6.0.1 https://github.com/bleachbit/bleachbit/security/advisories/GHSA-vciw-px28-5w94	poc	no	total
CVE-2026-81469	7,8	Dell Inventory Collector Client, versions	Unquoted Search Path or Element	versions prior to 15.0.0	https://www.dell.com/support/kbdoc/en-us/000502474/dsa-2026-381-security-update-for-dell-supportassist-for-pcs-home-and-business-dell-optimizer-dell-trusted-device-dell-command-update-for-an-unquoted-search-path-or-element-vulnerability			
CVE-2026-55105	7,7	Joplin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 3.6.15 and 3.7.2	https://github.com/laurent22/joplin/commit/8e0812de9d79d1f0698bb76a8c5d7e991df9748d https://github.com/laurent22/joplin/pull/15659 https://github.com/laurent22/joplin/security/advisories/GHSA-17a3-3qrx-6wg9			
CVE-2026-93991	7,7	Argo Workflows	Authorization Bypass Through User-Controlled Key	versions 4.1.0 through 4.1.3	https://github.com/argoproj/argo-workflows https://github.com/argoproj/argo-workflows/commit/a40972386c097ddf816d2e60e13f058bedca53d9 https://github.com/argoproj/argo-workflows/releases/tag/v4.1.4 https://github.com/argoproj/argo-workflows/security/advisories/GHSA-q65w-j2vp-47c4 https://www.vulncheck.com/advisories/argo-workflows-4.1.0-through-4.1.3-cross-namespace-disclosure-via-negated-selector	none	no	partial
CVE-2026-94540	7,7	DesktopSMS	Missing Authentication for Critical Function	1.11.0 and earlier	https://github.com/actuator/net.mrpearl.apps.desktopsmslite https://www.vulncheck.com/advisories/desktopsms-unauthorized-access-via-local-service			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-73512	7,5	Envoy	Use After Free	Prior to 1.36.10, 1.37.6, 1.38.4	https://github.com/envoyproxy/envoy/commit/29dbaee4a9971011e2f1948acfa383296e901ea https://github.com/envoyproxy/envoy/commit/85495163f4dc67364a5258bfe478c34a44f6428b4 https://github.com/envoyproxy/envoy/commit/c0e46dabc3ac286bbe608e9274776555911aadb9 https://github.com/envoyproxy/envoy/commit/f2417eec2ff49abe243d484ded916fbc2faca38d https://github.com/envoyproxy/envoy/releases/tag/v1.36.10 https://github.com/envoyproxy/envoy/releases/tag/v1.37.6			
CVE-2026-82560	7,5	Pod::Text versions	Loop with Unreachable Exit Condition ('Infinite Loop')	versions before 6.1.1	https://github.com/rra/podlators/commit/70510174f69eb54aa6d617bde4e1402cd9b7c61f.patch https://metacpan.org/release/RRA/podlators-v6.1.0/source/lib/Pod/Text.pm#L245-261 https://metacpan.org/release/RRA/podlators-v6.1.1/changes http://www.openwall.com/lists/oss-security/2026/09/19/6	none	yes	partial
CVE-2026-88407	7,5	the node_token_count/relation_token_count component of FalkorDB (Redis module)		v4.20.1 to v4.20.4	https://github.com/FalkorDB/FalkorDB/issues/2328			
CVE-2026-88411	7,5	the GRAPH			https://github.com/FalkorDB/FalkorDB/commit/17cb1f8f0 https://github.com/FalkorDB/FalkorDB/pull/2247			
CVE-2026-88806	7,5	libX11	Heap-based Buffer Overflow	before 1.8.14	https://gitlab.freedesktop.org/xorg/lib/libx11/-/merge_requests/309	none	no	total
CVE-2026-93990	7,5	Expat	Improper Handling of Unicode Encoding	through 2.8.4	https://github.com/libexpat/libexpat https://github.com/libexpat/libexpat/commit/ff6e1d7e750bbe245178f51a47a965dc8342861a https://github.com/libexpat/libexpat/pull/1282 https://www.vulncheck.com/advisories/expat-through-2.8.4-malformed-utf-16-acceptance-via-unchecked-surrogate	none	yes	partial
CVE-2026-94056	7,5	Exim	Use of Uninitialized Resource	before 4.100.1	https://lists.exim.org/turker/message/20260918.121220.0f87338e.en.html	none	no	partial
CVE-2026-94449	7,5	the SmallRye Fault Tolerance library	Uncontrolled Resource Consumption		https://access.redhat.com/security/cve/CVE-2026-94449 https://bugzilla.redhat.com/show_bug.cgi?id=2537502	none	yes	partial
CVE-2026-94622	7,5	vLLM versions	Uncaught Exception	through 0.29.0	https://github.com/vllm-project/vllm https://github.com/vllm-project/vllm/blob/v0.29.0/vllm/distributed/kv_transfer/kv_connector/v1/nixl/metadata.py#L294-L312 https://github.com/vllm-project/vllm/pull/54807 https://www.vulncheck.com/advisories/vllm-through-0.29.0-denial-of-service-via-incomplete-nixl-kv-transfer-metadata			
CVE-2026-94623	7,5	vLLM	Reachable Assertion	through 0.29.0	https://github.com/vllm-project/vllm https://github.com/vllm-project/vllm/blob/v0.29.0/vllm/distributed/kv_transfer/kv_connector/v1/nixl/base_worker.py#L2642-L2646 https://github.com/vllm-project/vllm/pull/51505 https://www.vulncheck.com/advisories/vllm-through-0.29.0-denial-of-service-via-nixl-multi-prompt-assertion-failure			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-94627	7,5	vLLM Mooncake connector	Missing Release of Memory after Effective Lifetime	through 0.29.0	https://github.com/vllm-project/vllm https://github.com/vllm-project/vllm/blob/v0.29.0/vllm/distributed/kv_transfer/kv_connector/v1/mooncake/mooncake_connector.py#L1978-L1989 https://github.com/vllm-project/vllm/pull/49796 https://www.vulncheck.com/advisories/vllm-through-0.29.0-gpu-kv-cache-leak-via-mooncake-transfer-id-collision			
CVE-2026-75939	7,4	openshift/oc-mirror	Improper Verification of Cryptographic Signature		https://access.redhat.com/security/cve/CVE-2026-75939 https://bugzilla.redhat.com/show_bug.cgi?id=2517976			
CVE-2026-94491	7,3	Yonyou KSOA	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')	9.0	https://vuldb.com/cve/CVE-2026-94491 https://vuldb.com/submit/895364 https://vuldb.com/vuln/408191 https://vuldb.com/vuln/408191/cti			
CVE-2025-71421	7,2	UVdesk core-framework	Improper Privilege Management	before 1.1.7	https://github.com/uvdesk/community-skeleton/releases/tag/v1.1.8 https://github.com/uvdesk/core-framework https://github.com/uvdesk/core-framework/blob/v1.1.6/Controller/Account.php#L278-L282 https://github.com/uvdesk/core-framework/commit/b8bcdc503659f9d5c5cd73627cfc5d45508b9a55 https://github.com/uvdesk/core-framework/releases/tag/v1.1.7 https://hackmd.io/@leedjy/B1Cz5voFGg	none	no	total
CVE-2026-36467	7,2	core/modules/media	Unrestricted Upload of File with Dangerous Type		https://github.com/CuteNews/cutenews-2.0 https://github.com/CuteNews/cutenews-2.0/blob/master/core/modules/media.php https://github.com/UmbraDeorum/cutenews-2.0-CVEs-2026-Disclosure	none	no	total
CVE-2026-61687	7,1	Hatchet	Improper Authentication; Cross-Site Request Forgery (CSRF); Session Fixation; Sensitive Cookie with Improper SameSite Attribute	Prior to 0.91.1	https://github.com/hatchet-dev/hatchet/commit/f90464189ad642251e09412d0f99fde353036428 https://github.com/hatchet-dev/hatchet/security/advisories/GHSA-phq3-3q28-wq9v	none	no	partial
CVE-2026-94368	7,1	the signature verification logic of noobaa-core, the core component of the NooBaa Multicloud Object Gateway	Improper Verification of Cryptographic Signature		https://access.redhat.com/security/cve/CVE-2026-94368 https://bugzilla.redhat.com/show_bug.cgi?id=2537364	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-2026-94534	7,1	lamp-cloud	Authorization Bypass Through User-Controlled Key	through 5.10.0	https://github.com/LinYuanvj1/cve-request-poc/blob/master/lamp/poc-03-anyone-baseinfo-write-bola.py https://github.com/LinYuanvj1/cve-request-poc/blob/master/lamp/poc-06-anyone-avatar-write-bola.py https://github.com/dromara/lamp-cloud/blob/bdc1a406eb0f6291e9f6dbad9cbccd67bc6a37b6/lamp-oauth/lamp-oauth-controller/src/main/java/top/tangyuh/lamp/oauth/controller/UserInfoController.java#L128-L136 https://github.com/dromara/lamp-cloud/blob/bdc1a406eb0f6291e9f6dbad9cbccd67bc6a37b6/lamp-oauth/lamp-oauth-controller/src/main/java/top/tangyuh/lamp/oauth/controller/UserInfoController.java#L68-L78 https://www.vulncheck.com/advisories/lamp-cloud-through-5.10.0-unauthorized-profile-modification-via-put-endpoints			

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-2026-7273 Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability	https://cisa.gov/news-events/alerts/2026/09/21/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
Hackers Impersonate IT Help Desk on Microsoft Teams to Steal Windows Passwords	https://cybersecuritynews.com/hackers-impersonate-it-help-desk-on-teams
US Proposes AI Incident Alert System in Talks With China, Bessent Says	https://securityweek.com/us-proposes-ai-incident-alert-system-in-talks-with-china-bessent-says
Microsoft to retire Microsoft 365 Companion apps in December	https://bleepingcomputer.com/news/microsoft/microsoft-to-retire-microsoft-365-companion-apps-in-december
Google Hit With \$463 Million Fine for EU Location Data Rule Breach	https://securityweek.com/google-hit-with-463-million-fine-for-eu-location-data-rule-breach
Google Fined €403 Million for GDPR Violations Over Users' Location Data	https://cybersecuritynews.com/google-fined-e403-million
AWS Automatically Quarantines Exposed IAM Keys Within 10 Seconds of GitHub Leak	https://cybersecuritynews.com/aws-automatically-quarantines-exposed-iam-keys
Claude Code Agent Allegedly Deletes 48,000 Files in 103 Seconds	https://cybersecuritynews.com/claude-code-agent-file-deletion
Google fined €403 million over location data privacy violations	https://bleepingcomputer.com/news/security/google-fined-403-million-over-location-data-privacy-violations
Google Hit with €403m GDPR Fine Over Location Data Practices	https://infosecurity-magazine.com/news/google-hit-with-403m-gdpr-fine
Microsoft Entra ID to Block SMS First-Factor Sign-Ins Worldwide in February 2027	https://cybersecuritynews.com/entra-id-sms-sign-in-retirement
New Exvicy ClickFix Framework Built on Rival ErrTraffic's Code	https://infosecurity-magazine.com/news/exvicy-clickfix-framework
CISO Conversations: Noopur Davis – The Accidental Global CISO at Comcast	https://securityweek.com/ciso-conversations-noopur-davis-the-accidental-global-ciso-at-comcast
Microsoft Investigating Teams Calling Issue Blocking Users From Making or Receiving Calls	https://cybersecuritynews.com/microsoft-teams-calling-issue
Dragos Completes NetRise and runZero Acquisitions Following Accenture Deal	https://securityweek.com/dragos-completes-netrise-and-runzero-acquisitions-following-accenture-deal
Attackers Abuse npm Trusted Publishing in GHAPPIER Campaign	https://infosecurity-magazine.com/news/attackers-abuse-npm-trusted
Microsoft Confirms September 2026 Windows Updates Break File History Backups	https://cybersecuritynews.com/windows-updates-breaks-file-history-backup
Microsoft reminds admins to migrate Entra ID users to passkeys	https://bleepingcomputer.com/news/microsoft/microsoft-reminds-admins-to-migrate-entra-id-users-to-passkeys
ChatGPT Ad Tracking Cookie Follows Users Across Third-Party Advertiser Websites	https://cybersecuritynews.com/chatgpt-ad-tracking-cookie-follows-users
RatHat Android Trojan Uses AI for Automation	https://securityweek.com/rathat-android-trojan-uses-ai-for-automation
Rust Team Members and Popular Crate Owners Targeted via Video Calls	https://securityweek.com/rust-team-members-and-popular-crate-owners-targeted-via-video-calls

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
BigCommerce alerts merchants of data breach linked to Ribon apps	https://bleepingcomputer.com/news/security/bigcommerce-alerts-merchants-of-data-breach-linked-to-ribon-apps
ShinyHunters Hacked Clop. Now What About Clop's Victims?	https://darkreading.com/cyberattacks-data-breaches/shinyhunters-hacked-clop-what-about-clops-victims
Google Gemini AI Hacked 3 Real Companies during a Cybersecurity Test	https://cybersecuritynews.com/google-gemini-ai-hacked-3-real-companies

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
WordPress Comment2Shell Flaw Can Turn Anonymous Comment XSS Into RCE via Admin Session	https://thehackernews.com/2026/09/wordpress-comment2shell-flaw-can-turn.html
Zyxel and Veeam Flaws Under Active Exploitation With Command and SYSTEM Access	https://thehackernews.com/2026/09/zyxel-and-veeam-flaws-under-active.html
CISA alerts of active exploitation of three Linux kernel flaws	https://bleepingcomputer.com/news/security/cisa-alerts-of-active-exploitation-of-three-linux-kernel-flaws
WordPress Click2Shell flaw lets hackers execute PHP on the server	https://bleepingcomputer.com/news/security/wordpress-click2shell-flaw-lets-hackers-execute-php-on-the-server
⚡ Weekly Recap: Cisco 0-Day, AI Agent RCE, ClickFix Attacks, ClickFix Surge, and Browser Hijacks	https://thehackernews.com/2026/09/weekly-recap-cisco-0-day-ai-agent-rce.html
Organizations Warned of 3 Exploited Linux Kernel Vulnerabilities	https://securityweek.com/organizations-warned-of-3-exploited-linux-kernel-vulnerabilities
MSNightmare Releases New PoC for DoS Vulnerability in Windows Defender	https://cybersecuritynews.com/defender-bigdiskbuster-dos-flaw
Weekly Cybersecurity Newsletter Bulletin - Cisco and Android 0-Day, BragJack Attack, Claude Opus 5 Used to Hack OpenAI, and 20+ Stories	https://cybersecuritynews.com/weekly-cybersecurity-newsletter-sept-21
Claude Opus 5 Helped Researchers Take Over OpenAI Staff Accounts via Chained Flaws	https://thehackernews.com/2026/09/claude-opus-5-helped-researchers-take.html
CISA Warns of Linux Kernel Vulnerabilities Actively Exploited in Attacks	https://cybersecuritynews.com/linux-kernel-vulnerabilities-actively-exploited
Critical Pre-Auth RCE in Orkes Conductor Workflow Platform Exploited in the Wild	https://thehackernews.com/2026/09/critical-pre-auth-rce-in-orkes.html
CISA Flags Three Linux Kernel Vulnerabilities Exploited in the Wild	https://thehackernews.com/2026/09/cisa-flags-three-linux-kernel.html

Click2Shell WordPress Flaw Lets Attackers Gain RCE With a Single Malicious Link	https://cybersecuritynews.com/click2shell-wordpress-vulnerability
---	---

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
Microsoft fixes broken Excel copy and paste for all Office users	https://bleepingcomputer.com/news/microsoft/microsoft-fixes-broken-excel-copy-and-paste-for-all-office-users
SolarWinds Patches ARM Hard-Coded Key Flaw Enabling Unauthenticated RCE	https://thehackernews.com/2026/09/solarwinds-patches-arm-hard-coded-key.html

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
Meta's Muse AI Agent 0-Day Vulnerability Allows Attackers to Hijack the Tool and Inject Malware	https://cybersecuritynews.com/metasploit-muse-ai-agent-0-day-vulnerability
Cybercriminals Hiding New Malware in Torrents for Popular Films	https://darkreading.com/cyberattacks-data-breaches/cybercriminals-hiding-new-malware-torrents-popular-films
Fake LastPass Installers Push Kernel-Level EDR Killer, 'Rapuncel' Stealer	https://securityweek.com/fake-lastpass-installers-push-kernel-level-edr-killer-rapuncel-stealer
PAYLOAD Ransomware Hijacks Active Directory GPO to Disrupt Entire Windows Domain Without Encryption	https://cybersecuritynews.com/payload-ransomware-hijacks-active-directory
Malicious npm Package With 2 Million Downloads Hides Malware in Runtime Code	https://cybersecuritynews.com/malicious-npm-package
ShinyHunters Claim Hack of Rival Ransomware Gang Clop	https://infosecurity-magazine.com/news/shinyhunters-claim-hack-of-clop
CrowdSec Confirms Source Code Stolen in Supply Chain Attack	https://securityweek.com/crowdsec-confirms-source-code-stolen-in-supply-chain-attack
Hackers Hide Malware Servers on Blockchain to Steal Bank Logins and 2FA Codes	https://cybersecuritynews.com/hackers-hide-malware-servers
Hackers Exploit cPanel CVE-2026-41940 Auth Bypass to Deploy Mirai Malware	https://cybersecuritynews.com/cpanel-cve-2026-41940
Revolut Customers Targeted with New Wave of Phishing Attacks	https://infosecurity-magazine.com/news/revolut-customers-targeted-wave

Σύντομη περιγραφή / Τίτλος	URL
New Android Malware Uses AI to Steal Bank Logins and Reconstruct Your PIN	https://cybersecuritynews.com/android-malware-uses-ai
Malicious npm packages evade install-script defenses at runtime	https://bleepingcomputer.com/news/security/malicious-npm-packages-evade-install-script-defenses-at-runtime
When Ransomware Targets AI Models: Defending the AI/ML Recovery Chain	https://cybersecuritynews.com/when-ransomware-targets-ai-models-defending-the-ai-ml-recovery-chain
ShinyHunters hacks Clop leak site, threatens to extort ransomware gang	https://bleepingcomputer.com/news/security/shinyhunters-hacks-clop-leak-site-threatens-to-extort-ransomware-gang
TanStack Supply Chain Attack Lets Hackers Steal 170 Private CrowdSec GitHub Repositories	https://cybersecuritynews.com/tanstack-supply-chain-attack

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
How AI Agents Can Trigger Runaway Costs for Enterprises	https://darkreading.com/application-security/how-ai-agents-can-trigger-runaway-costs

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 19/09/2026–22/09/2026, και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

Annex – Websites with vendor specific vulnerabilities

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

Vendor name / Platform	URL
Wordpress	Wordfence Intelligence Vulnerability Database API 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/