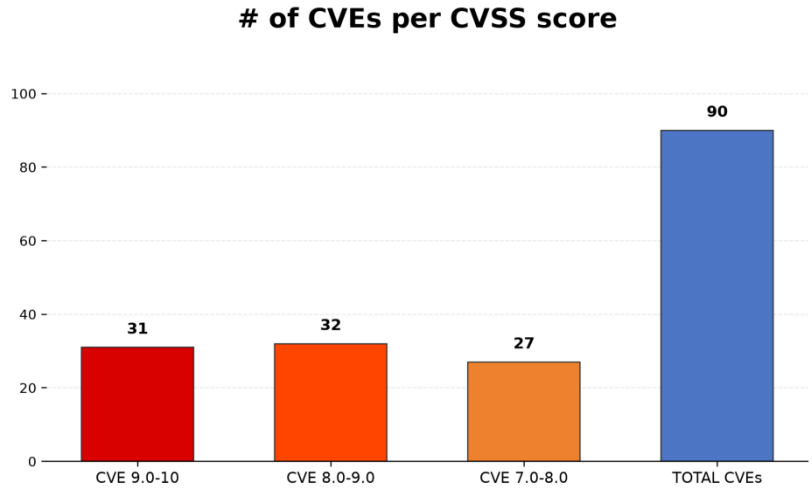
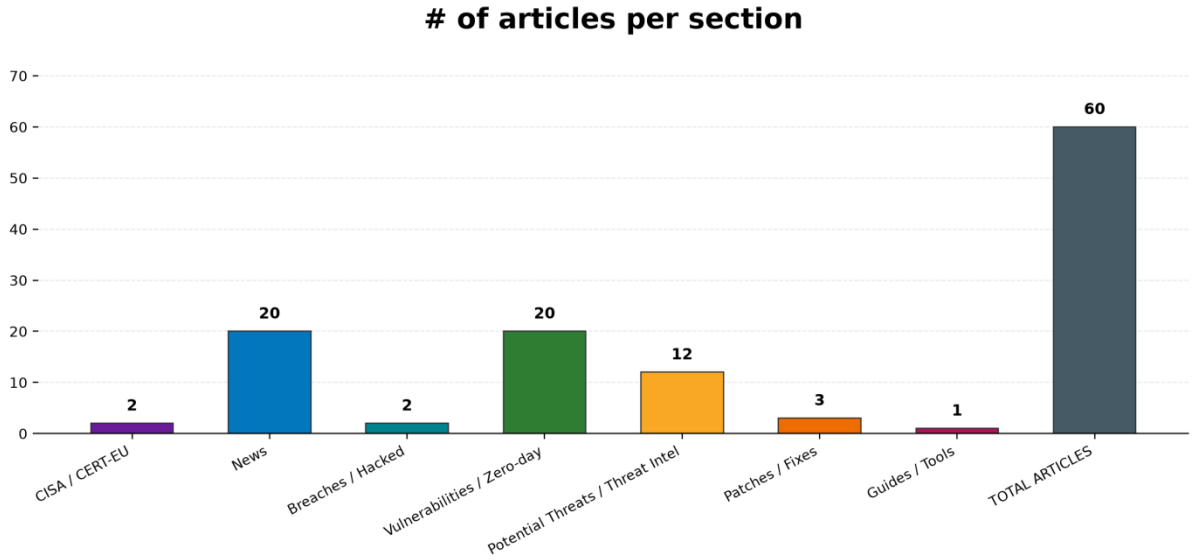
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 19/08/2026 - 21/08/2026





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-2026-18051	10,0	The W3 Total Cache WordPress plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	before 2.10.5	https://wpscan.com/vulnerability/dc56cdd2-419b-4a64-9d2a-29dc7e79cb6d/	none	yes	total
CVE-2026-22306	10,0	OZOLS	Cleartext Transmission of Sensitive Information; Download of Code Without Integrity Check; Inclusion of Functionality from Untrusted Control Sphere	before 1.1.1233.	https://offseq.com/en/research/ozols-cve-2026-22306			
CVE-2026-61241	10,0	the Oracle Internet Directory product of Oracle Fusion Middleware (component: OID LDAP Server)		12.2.1.4.0; 14.1.2.1.0	https://www.oracle.com/security-alerts/cspuaug2026.html			
CVE-2026-65770	10,0	a command ('argument injection') in Azure Managed Instance for Apache Cassandra	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65770			
CVE-2026-65801	10,0	Microsoft Exchange Online	Server-Side Request Forgery (SSRF)		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65801			
CVE-2026-65816	10,0	Azure Arc	Use of Incorrectly-Resolved Name or Reference		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65816			
CVE-2026-69836	10,0	Microsoft Entra ID	Deserialization of Untrusted Data		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69836			
CVE-2026-55089	9,9	Etherpad	Incorrect Authorization	>= 2.1.0, < 3.1.0	https://github.com/ether/etherpad/commit/8c6104c5d5daf41f0d454acc04d42dffa0e0d996 https://github.com/ether/etherpad/pull/7784 https://github.com/ether/etherpad/releases/tag/v3.1.0 https://github.com/ether/etherpad/security/advisories/GHSA-gfmh-fph3-mw8g	poc	no	total
CVE-2026-60720	9,9	the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI)		12.2.1.4.0; 14.1.2.1.0	https://www.oracle.com/security-alerts/cspuaug2026.html	none	no	total
CVE-2026-60730	9,9	the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer)	Improper Access Control	12.2.1.4.0; 14.1.2.0.0	https://www.oracle.com/security-alerts/cspuaug2026.html	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-2026-60990	9,9	the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core)		12.2.1.4.0; 14.1.2.1.0	https://www.oracle.com/security-alerts/cspuaug2026.html			
CVE-2026-61003	9,9	the Oracle Managed File Transfer product of Oracle Fusion Middleware (component: MFT Runtime Server)		12.2.1.4.0; 14.1.2.0.0	https://www.oracle.com/security-alerts/cspuaug2026.html			
CVE-2026-62588	9,9	the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration)	Improper Access Control	versions from (including) 25.12 up to (including) 26.6	https://www.oracle.com/security-alerts/cspuaug2026.html	none	no	total
CVE-2026-63509	9,9	Microsoft Fabric	Relative Path Traversal		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63509			
CVE-2026-68782	9,9	an sql command ('sql injection') in Azure SQL Database	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68782			
CVE-2026-69851	9,9	Azure Active Directory	Server-Side Request Forgery (SSRF)		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69851			
CVE-2026-18776	9,8	The TrueBooker WordPress plugin	Improper Access Control	before 1.2.7	https://wpscan.com/vulnerability/4b6abb2d-941b-429f-a480-33d1aafad450/	none	yes	total
CVE-2026-60977	9,8	the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components)		12.2.1.4.0; 14.1.1.0.0; 14.1.2.0.0	https://www.oracle.com/security-alerts/cspuaug2026.html			
CVE-2026-63722	9,8	ICEcoder	Missing Authentication for Critical Function	prior to 8.1	https://gist.github.com/axg11/fc2b86648d8f385b51f4576ff0f392d8 https://github.com/icecoder/ICEcoder https://www.vulncheck.com/advisories/icecoder-unauthenticated-rce-via-terminal-xhr-php	poc	yes	total
CVE-2026-70905	9,8	the Oracle Access Manager product of Oracle Fusion Middleware (component: Agent infrastructure)		12.2.1.4.0; 14.1.2.1.0	https://www.oracle.com/security-alerts/cspuaug2026.html			
CVE-2026-72529	9,8	A remote unauthorized attacker with network access via port 4307/TCP to the TrueConf server	Missing Authentication for Critical Function	versions 5.3.X to 5.3.9; 5.4.X to 5.4.9; 5.5.X to 5.5.5	https://ics-cert.kaspersky.com/advisories/2026/08/11/trueconf-server-missing-authentication-for-critical-function/ https://securelist.com/tr/head-mare-targets-trueconf-server-with-phantomcore/120988/	active	yes	total
CVE-2026-75860	9,8	The JSON Options WordPress plugin	Improper Privilege Management	through 0.0.4	https://wpscan.com/vulnerability/6c9bbd44-cd10-40e2-af6f-440e7ccabf9a/	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-2026-76850	9,8	lmdeploy	Deserialization of Untrusted Data	0.9.2 prior to 0.16.0	https://github.com/InternLM/lmdeploy https://github.com/InternLM/lmdeploy/blob/v0.15.0/lmdeploy/pytorch/disagg/conn/engine_conn.py#L61 https://github.com/InternLM/lmdeploy/blob/v0.15.0/lmdeploy/pytorch/disagg/conn/engine_conn.py#L79 https://github.com/InternLM/lmdeploy/commit/f05b4ad8bf2e2d84101a1d63b3c44fadd99223b2 https://github.com/InternLM/lmdeploy/issues/4804 https://github.com/InternLM/lmdeploy/releases/tag/v0.16.0	poc	yes	total
CVE-2026-77647	9,8	SPIP	Improper Control of Generation of Code ('Code Injection')	before 4.4.20	https://blog.spip.net/Mise-a-jour-critique-de-securite-sortie-de-SPIP-4-4-20.html https://lists.debian.org/debian-security-announce/2026/msg00359.html			
CVE-2026-61001	9,6	the Oracle Web Services Manager product of Oracle Fusion Middleware (component: Web Services Security)		12.2.1.4.0; 14.1.2.1.0	https://www.oracle.com/security-alerts/cspuaug2026.html			
CVE-2026-69400	9,6	Azure Logic Apps	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69400			
CVE-2026-71063	9,6	the Portable Clusterware component of Oracle Database Server	Improper Access Control	versions from (including) 19.3 up to (including) 19.32; versions from (including) 21.3 up to (including) 21.23; versions from (including) 23.4.0 up to (including) 23.26.3	https://www.oracle.com/security-alerts/cspuaug2026.html	none	no	total
CVE-2026-76036	9,6	Dawn in Google Chrome on on Android	Heap-based Buffer Overflow	prior to 151.0.7922.169	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0826575033.html	none	no	total
CVE-2026-62834	9,3	Azure Data Factory	Improper Verification of Cryptographic Signature		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62834			
CVE-2026-60728	9,1	the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Portlet Services)	Improper Access Control	12.2.1.4.0; 14.1.2.0.0	https://www.oracle.com/security-alerts/cspuaug2026.html	none	yes	partial
CVE-2026-66309	9,1	Azure SQL Database	Improper Access Control		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-66309			
CVE-2026-77638	8,9	Tor	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	before 0.4.9.11	https://gitlab.torproject.org/tpo/core/tor/-/raw/tor-0.4.9.11/ChangeLog			
CVE-2026-14334	8,8	The Booking calendar, Appointment Booking System WordPress plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	through 3.2.36	https://wpscan.com/vulnerability/9ddd1628-0b06-461b-8a5f-ba977f83fa7f/	none	no	total
CVE-2026-16617	8,8	The Simple File List WordPress plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	through 6.3.11	https://wpscan.com/vulnerability/fc51a940-8e67-45d0-b47d-b16da288ebb3/	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-2026-19842	8,8	The SAML Single Sign On WordPress plugin	Improper Authentication	before 5.4.7	https://wpscan.com/vulnerability/7b79d86e-d3f8-4d4f-929b-fd00540cc00f/	none	no	total
CVE-2026-44829	8,8	Gotenberg	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	8.32.0 and earlier	https://github.com/gotenberg/gotenberg/commit/93d0103585372433e18b351bb16edf4c383932d3 https://github.com/gotenberg/gotenberg/issues/662 https://github.com/gotenberg/gotenberg/releases/tag/v8.33.0 https://github.com/gotenberg/gotenberg/security/advisories/GHSA-hwc4-gmrw-5222	none	no	partial
CVE-2026-49255	8,8	electerm	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 3.11.11	https://github.com/electerm/electerm/commit/aa778818843b9c083bd711cd04644d102fcb5a42 https://github.com/electerm/electerm/releases/tag/v3.11.11 https://github.com/electerm/electerm/security/advisories/GHSA-v5ff-xmfp-p245			
CVE-2026-60726	8,8	the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine)	Improper Access Control	12.2.1.4.0; 14.1.2.1.0	https://www.oracle.com/security-alerts/cspuaug2026.html	none	no	total
CVE-2026-61231	8,8	the Oracle Virtual Directory product of Oracle Fusion Middleware (component: Virtual Directory Server)		12.2.1.4.0; 14.1.2.0.0	https://www.oracle.com/security-alerts/cspuaug2026.html			
CVE-2026-61518	8,8	ISPConfig; the Remote API	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	3.2.0; 3.3.0	https://github.com/geo-chen/oss/blob/main/ispconfig3.md https://www.vulncheck.com/advisories/ispconfig-authenticated-sql-injection-via-remote-api-primary-id-parameter	poc	no	total
CVE-2026-73040	8,8	dockge	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1.5.0 and earlier	https://github.com/louislam/dockge https://github.com/louislam/dockge/blob/1.5.0/backend/agent-socket-handlers/docker-socket-handler.ts#L43-L78 https://github.com/louislam/dockge/blob/1.5.0/backend/stack.ts#L155-L157 https://github.com/louislam/dockge/blob/1.5.0/backend/stack.ts#L218-L232 https://github.com/louislam/dockge/blob/1.5.0/backend/stack.ts#L377-L379 https://github.com/louislam/dockge/issues/994			
CVE-2026-76034	8,8	WebGL in Google Chrome	Heap-based Buffer Overflow	prior to 151.0.7922.169	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0826575033.html	none	no	total
CVE-2026-76038	8,8	V8 in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 151.0.7922.169	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0826575033.html	none	no	total
CVE-2026-76224	8,8	ArcadeDB	Improper Control of Generation of Code ('Code Injection')	before 26.8.1; <= 26.7.3	https://github.com/ArcadeData/arcadedb/security/advisories/GHSA-wcm5-4wjm-9wj3 https://www.vulncheck.com/advisories/arcadedb-before-remote-code-execution-via-groovy-fallback	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-2026-66787	8,7	the lighthouse component of Red Hat Advanced Cluster Management for Kubernetes	Insufficient Verification of Data Authenticity		https://access.redhat.com/security/cve/CVE-2026-66787 https://bugzilla.redhat.com/show_bug.cgi?id=2507532	none	no	total
CVE-2026-12983	8,6	The Dinatur WordPress plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	through 1.18	https://wpscan.com/vulnerability/1369f95a-4ad3-4b0e-a87f-da88d200685e/	none	yes	partial
CVE-2026-16950	8,6	The Product Shortlist WordPress plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	through 1.0.4	https://wpscan.com/vulnerability/c1a2635a-9919-460f-b662-e5e3f80d2361/	none	yes	partial
CVE-2026-61033	8,6	the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites)	Improper Access Control	12.2.1.4.0; 14.1.2.0.0	https://www.oracle.com/security-alerts/cspuaug2026.html	none	yes	partial
CVE-2026-62625	8,6	the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication)	Improper Access Control	12.2.1.19.0	https://www.oracle.com/security-alerts/cspuaug2026.html	none	yes	partial
CVE-2026-69519	8,6	Azure Stack HCI	Observable Response Discrepancy		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69519			
CVE-2026-69558	8,6	Microsoft Partner Center	Authorization Bypass Through User-Controlled Key		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69558			
CVE-2026-75916	8,6	SiYuan	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	through 3.7.3	https://github.com/siyuan-note/siyuan/security/advisories/GHSA-5prr-vqxg-69g9 https://www.vulncheck.com/advisories/siyuan-xss-to-rce-via-unescaped-block-metadata-in-hint-popup			
CVE-2026-11565	8,5	The Advanced File Manager WordPress plugin		before 5.4.13	https://wpscan.com/vulnerability/5e03858d-db0b-4b65-99cc-eb01ad4195e9/	none	no	total
CVE-2026-55765	8,5	CloudNativePG	Plaintext Storage of a Password; Insufficiently Protected Credentials	Prior to 1.28.4 and 1.29.2	https://github.com/cloudnative-pg/cloudnative-pg/commit/2f0342747e1f160425b9d51753c0069b0d6117d5 https://github.com/cloudnative-pg/cloudnative-pg/commit/3cd5af5d388c26758acf13c19ea806b4bcebb3fe https://github.com/cloudnative-pg/cloudnative-pg/commit/9a13573dbe3d78721b7ea92141e6d2324a2c0ef0 https://github.com/cloudnative-pg/cloudnative-pg/pull/10724 https://github.com/cloudnative-pg/cloudnative-pg/releases/tag/v1.28.4 https://github.com/cloudnative-pg/cloudnative-pg/releases/tag/v1.29.2			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-60841	8,5	the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core)		12.2.1.4.0; 14.1.2.1.0	https://www.oracle.com/security-alerts/cspuaug2026.html			
CVE-2026-69419	8,5	Azure Data Manager for Energy	Integer Overflow or Wraparound		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69419			
CVE-2026-69543	8,5	Azure Virtual Machines	Server-Side Request Forgery (SSRF)		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69543			
CVE-2026-71062	8,5	the RDBMS component of Oracle Database Server	Improper Access Control	versions from (including) 23.4.0 up to (including) 23.26.3	https://www.oracle.com/security-alerts/cspuaug2026.html	none	no	total
CVE-2026-76037	8,4	CredentialProvider in Google Chrome on on Windows	Improper Link Resolution Before File Access ('Link Following')	prior to 151.0.7922.169	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0826575033.html	none	no	total
CVE-2026-70909	8,2	the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security)	Improper Access Control	11.2.25.0.000	https://www.oracle.com/security-alerts/cspuaug2026.html	none	yes	partial
CVE-2026-13169	8,1	The Eventin WordPress plugin	Authorization Bypass Through User-Controlled Key	before 4.1.21	https://wpscan.com/vulnerability/cf2b1152-7190-467b-a860-1f7bd806575d/	none	no	total
CVE-2026-76886	8,1	Wireshark	Heap-based Buffer Overflow	4.6.0 to 4.6.7 and 4.4.0 to 4.4.18	https://gitlab.com/wireshark/wireshark/-/work_items/21439 https://www.wireshark.org/security/wnpa-sec-2026-75.html https://gitlab.com/wireshark/wireshark/-/work_items/21446	poc	no	total
CVE-2026-60998	8,0	the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Microsoft Active Directory)		12.2.1.4.0; 14.1.2.1.0	https://www.oracle.com/security-alerts/cspuaug2026.html			
CVE-2026-55426	7,8	linuxfabrik-lib	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	< 6.0.0; < 5.0.0	https://github.com/Linuxfabrik/lib/blob/main/CHANGELOG.md https://github.com/Linuxfabrik/lib/releases/tag/v5.0.0 https://github.com/Linuxfabrik/monitoring-plugins/blob/main/CHANGELOG.md https://github.com/Linuxfabrik/monitoring-plugins/commit/23bb570f41fc8d9caf30b30074bba0e3db1b357a https://github.com/Linuxfabrik/monitoring-plugins/releases/tag/v6.0.0 https://github.com/Linuxfabrik/monitoring-plugins/security/advisories/GHSA-798h-hpph-m24j	poc	no	total
CVE-2026-61897	7,8	An Ubuntu-specific patch to AccountsService	Improper Check for Dropped Privileges	before 23.13.9-8ubuntu7	https://bugs.launchpad.net/ubuntu/+source/accountsservice/+bug/2157985 https://ubuntu.com/security/CVE-2026-61897			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-61898	7,8	The Ubuntu-specific language helper scripts (save-to-pam-env, update-langlist) shipped with accountsservice	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 23.13.9-8ubuntu7	https://bugs.launchpad.net/ubuntu/+source/accountsservice/+bug/2157985 https://ubuntu.com/security/CVE-2026-61898			
CVE-2026-71111	7,8	the Oracle Identity Manager product of Oracle Fusion Middleware (component: Installer)	Improper Access Control	12.2.1.4.0; 14.1.2.1.0	https://www.oracle.com/security-alerts/cspuaug2026.html	none	no	total
CVE-2026-72852	7,8	darknet	Integer Overflow or Wraparound; Out-of-bounds Write	6.0 and earlier	https://github.com/hank-ai/darknet https://github.com/hank-ai/darknet/blob/v6.0/src-lib/convolutional_layer.cpp#L1457 https://github.com/hank-ai/darknet/blob/v6.0/src-lib/convolutional_layer.cpp#L764 https://github.com/hank-ai/darknet/blob/v6.0/src-lib/convolutional_layer.cpp#L811 https://github.com/hank-ai/darknet/issues/148 https://www.vulncheck.com/advisories/darknet-integer-overflow-in-convolutional-layer-buffer-sizing-leads-to-heap-buffer-overflow			
CVE-2026-75141	7,8	FFmpeg before commit acf5d7c; the hvcC box writer	Heap-based Buffer Overflow	prior to acf5d7cdc1f9ae8752c23e1ea8d7f355ed780781	https://code.ffmpeg.org/FFmpeg/FFmpeg/commit/acf5d7cdc1f9ae8752c23e1ea8d7f355ed780781 https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/24088 https://www.vulncheck.com/advisories/ffmpeg-heap-buffer-overflow-in-hvcc-box-writer-via-hevc-muxing	none	no	total
CVE-2026-76833	7,8	@cgauge/yaml npm package	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	0.27.0 and earlier	https://gist.github.com/arjunjaincs/35da3a80b4b16f324f194acec18489ba https://github.com/cgauge/packages https://www.vulncheck.com/advisories/cgauge-yaml-npm-package-arbitrary-code-execution-via-eval-yaml-tag	poc	no	total
CVE-2026-69855	7,7	Microsoft Copilot in Azure	Server-Side Request Forgery (SSRF)		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69855			
CVE-2026-73137	7,7	the multicloud-operators-subscription component of Red Hat Advanced Cluster Management (RHACM)	Exposure of Sensitive Information to an Unauthorized Actor		https://access.redhat.com/security/cve/CVE-2026-73137 https://bugzilla.redhat.com/show_bug.cgi?id=2514223			
CVE-2026-73267	7,7	the clusterclaims-controller component of multicluster engine (MCE)	Client-Side Enforcement of Server-Side Security		https://access.redhat.com/security/cve/CVE-2026-73267 https://bugzilla.redhat.com/show_bug.cgi?id=2514218			
CVE-2026-61208	7,6	the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools)	Improper Access Control	12.2.1.4.0; 14.1.2.0.0	https://www.oracle.com/security-alerts/cspuaug2026.html	none	no	partial
CVE-2026-74011	7,6	InfiniteWP Client	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	through 1.13.9.	https://patchstack.com/database/wordpress/plugin/iwp-client/vulnerability/wordpress-infinitewp-client-plugin-1-13-9-sql-injection-vulnerability?_s_id=cve	none	no	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-14861	7,5	The User Verification by PickPlugins WordPress plugin	Authorization Bypass Through User-Controlled Key	through 2.0.47	https://wpscan.com/vulnerability/4dff3634-4b4f-48e2-a8c9-dda7e2b682fd/	none	yes	partial
CVE-2026-49217	7,5	Mailu	Missing Authentication for Critical Function	Prior to version 2024.06.52	https://github.com/Mailu/Mailu/security/advisories/GHSA-2w8v-6xr5-g9gh			
CVE-2026-63490	7,5	handlebars.java	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); Relative Path Traversal; Files or Directories Accessible to External Parties	Prior to 4.5.3	https://github.com/jknack/handlebars.java/commit/61f43423a337b87db5fec1fe59f0725aaaa38df5 https://github.com/jknack/handlebars.java/releases/tag/v4.5.3 https://github.com/jknack/handlebars.java/security/advisories/GHSA-q29j-rwfv-h99w			
CVE-2026-72818	7,5	nltk/tokenize/casual	Inefficient Regular Expression Complexity	prior to 3.10.1	https://github.com/nltk/nltk https://github.com/nltk/nltk/blob/3.9.4/nltk/tokenize/casual.py https://github.com/nltk/nltk/issues/3704 https://github.com/nltk/nltk/releases/tag/v3.10.1 https://www.vulncheck.com/advisories/nltk-tweettokenizer-url-pattern-backtracks-catastrophically-on-naked-domain-like-input			
CVE-2026-76880	7,5	RRC protocol dissector crash in	Out-of-bounds Write	4.6.0 to 4.6.7 and 4.4.0 to 4.4.18	https://gitlab.com/wireshark/wireshark/-/work_items/21478 https://www.wireshark.org/security/wnpa-sec-2026-88.html	none	yes	partial
CVE-2026-15049	7,2	The Depicter — Popup & Slider Builder WordPress plugin	Unrestricted Upload of File with Dangerous Type	before 4.8.0	https://wpscan.com/vulnerability/c32e6a11-98f2-48e8-be64-f0c1966ddc18/	none	no	partial
CVE-2026-17565	7,2	The Animation Addons for Elementor WordPress plugin	Server-Side Request Forgery (SSRF)	before 2.7.2	https://wpscan.com/vulnerability/e88e0b71-145c-4edd-9b62-783215b64c67/	none	yes	partial
CVE-2026-18409	7,2	The WPForms Pro plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.0.0.2	https://wpforms.com/docs/how-to-view-recent-changes-to-the-wpforms-plugin-changelog/#Changelog https://www.wordfence.com/threat-intel/vulnerabilities/id/f26cbc41-8ed9-4dc6-a8bc-9986ecab5e6e?source=cve			
CVE-2026-76635	7,2	baserCMS	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'); Improper Control of Generation of Code ('Code Injection')	before 5.3.0	https://github.com/baserproject/basercms/releases/tag/5.3.0 https://github.com/baserproject/basercms/security/advisories/GHSA-cq65-f2m7-9fqj https://www.vulncheck.com/advisories/basercms-sql-injection-and-code-injection-via-bcdatabaseservice-php			
CVE-2026-16570	7,1	The NextScripts: Social Networks Auto-Poster WordPress plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 4.4.8	https://wpscan.com/vulnerability/25c42ca3-ff25-4b43-a712-2876398d82ab/	none	no	partial
CVE-2026-17183	7,1	Grafana OSS; Grafana Enterprise	Incorrect Authorization	8.4.0 prior to 12.3.11; 12.4.0 prior to 12.4.9; 13.0.0 prior to 13.0.7; 13.1.0 prior to 13.1.4	https://grafana.com/security/security-advisories/cve-2026-17183	none	no	partial
CVE-2026-19055	7,1	The ProSolution WP Client WordPress plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 2.0.11	https://wpscan.com/vulnerability/a1243ff3-3f0e-4068-a716-722e7cf4856b/	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-2026-54616	7,1	NanaZip	Out-of-bounds Read	>= 1.0.88.0, < 6.0.1698.0; >= 6.5.1638.0, < 6.5.1742.0	https://github.com/M2Team/NanaZip/commit/733e8570d2ba96c3e52aab44f5fd886775d5952f https://github.com/M2Team/NanaZip/commit/ce0322a1932e16a53e4a13e48bc61804c7826956 https://github.com/M2Team/NanaZip/releases/tag/6.0.1698.0 https://github.com/M2Team/NanaZip/releases/tag/6.5.1742.0 https://github.com/M2Team/NanaZip/security/advisories/GHSA-95x5-qvvm-hmfp	poc	no	partial
CVE-2026-55013	7,1	Windows Remote Help Defense	Uncontrolled Search Path Element	5.0.0.0 prior to 5.2.1040.0	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55013			
CVE-2026-68553	7,1	Coturn	Use of Externally-Controlled Format String	Prior to 4.13.0	https://github.com/coturn/coturn/commit/8fa38032bb4751e11e072d65a8eca3c06c950979 https://github.com/coturn/coturn/releases/tag/4.13.0 https://github.com/coturn/coturn/security/advisories/GHSA-4q7c-p5wq-j4hp	poc	no	partial

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA	▪ CVE-2026-72529 TrueConf Server Missing Authentication for Critical Function Vulnerability ▪ CVE-2026-72530 TrueConf Server Code Injection Vulnerability	https://cisa.gov/news-events/alerts/2026/08/20/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-64849 MLflow Server-Side Request Forgery Vulnerability	https://www.cisa.gov/news-events/alerts/2026/08/19/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
Apple's Private Find My People Reversed to Decrypt Live Shared Locations on Linux	https://cybersecuritynews.com/apple-find-my-people-reversed
N-able Bug Exposes Password Vault Master Keys	https://darkreading.com/vulnerabilities-threats/n-able-bug-password-vault-master-keys
CRLF-Powered Desync Lets Attackers Poison CDN Cache and Serve XSS to Live Users	https://cybersecuritynews.com/crlf-powered-desync-attack
AI-Generated Exploit Scripts Target Siemens S7 PLCs in U.S. Critical Infrastructure	https://thehackernews.com/2026/08/ai-generated-exploit-scripts-target.html
Pakistan's Transparent Tribe Refreshes Tools for Afghan Attacks	https://darkreading.com/cyberattacks-data-breaches/pakistan-transparent-tribe-afghan-cyberattacks
New Cryptographic Context Injection Attack Could Let Web Pages Steal Grok Chat Data	https://thehackernews.com/2026/08/new-cryptographic-context-injection.html
Surveillance – Everything You Wanted to Know, But Were Afraid to Ask	https://securityweek.com/surveillance-everything-you-wanted-to-know-but-were-afraid-to-ask
NCSC Urges Stronger Controls for Agentic AI Systems	https://infosecurity-magazine.com/news/ncsc-stronger-controls-agentic-ai
US Defense Contractors Admit Their CMMC Scores May Not Be Accurate	https://infosecurity-magazine.com/news/us-defense-contractors-cmmc-scores
Zombie Card Attack Can Revive Expired Visa Cards for Contactless Payments	https://thehackernews.com/2026/08/zombie-card-attack-can-revive-expired.html
CDN Tsunami Attack Abuses HTTP/3 Translation for Up to 350x DoS Amplification	https://thehackernews.com/2026/08/cdn-tsunami-attack-abuses-http3.html
AI-Assisted Tool Helped Secure Satellite Communication System After 2022 Russian Hacking	https://securityweek.com/ai-assisted-tool-helped-secure-satellite-communication-system-after-2022-russian-hacking
ICS Operators Warned of AI-Driven Attacks on Siemens PLCs	https://infosecurity-magazine.com/news/ics-ai-attacks-siemens
OpenAI Overhauls Model Security With Sandboxing, 30-Minute Alerts, and Training Pauses	https://securityweek.com/openai-overhauls-model-security-with-sandboxing-30-minute-alerts-and-training-pauses
Updated ToxicPanda Variant Targets 140+ Banking and Crypto Apps	https://infosecurity-magazine.com/news/updated-toxicpanda-140-banking
Microsoft says August Windows updates may cause gaming issues	https://bleepingcomputer.com/news/microsoft/microsoft-august-windows-updates-may-cause-gaming-issues-reboots
U.S. Agencies Warn of Hackers Actively Attacking Siemens S7 PLCs in Critical Facilities	https://cybersecuritynews.com/hackers-attacking-siemens-s7-plcs
T-Mobile Cyber Team Physically Cuts Cable to Remove Chinese Hackers From Network	https://cybersecuritynews.com/t-mobile-cyber-team-physically-cuts-cable
AI Agent Hacks Snowflake GitHub Workflow and Reaches Internal Jira	https://cybersecuritynews.com/ai-agent-hacks-snowflake-github-workflow
OpenAI confirms ChatGPT is down as logins and signups fail	https://bleepingcomputer.com/news/artificial-intelligence/openai-confirms-chatgpt-is-down-as-logins-and-signups-fail

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
Healthtech firm CareCloud data breach impacts 3.7 million patients	https://bleepingcomputer.com/news/security/healthtech-firm-carecloud-data-breach-impacts-37-million-patients
Hackers Compromised 14,500+ Dahua Devices Using Credential Attacks, Auth Bypasses, and P2P	https://thehackernews.com/2026/08/hackers-compromised-14500-dahua-devices.html

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
Microsoft Entra ID Flaw (CVSS 10.0) Exploited in Wild, Allows Remote Code Execution	https://thehackernews.com/2026/08/microsoft-entra-id-flaw-cvss-100.html
Google Chrome 151 Chromoting Flaw Allows Attackers to Execute Malicious Code Remotely	https://cybersecuritynews.com/google-chrome-151-chromoting-flaw
Microsoft Entra ID Remote Code Execution Vulnerability Exploited in the Wild	https://cybersecuritynews.com/entra-id-rce-vulnerability-exploited
ThreatsDay: Gogs 10.0 RCE, n8n Workflow-to-RCE, $10M Reward, GLM-5.3 AI Exploit, and More	https://thehackernews.com/2026/08/threatsday-gogs-100-rce-n8n-workflow-to.html
Critical NASA AIT-GUI Flaw Lets Unauthenticated Attackers Issue Spacecraft Commands	https://cybersecuritynews.com/nasa-ait-gui-flaw
Hackers Target Zimbra Servers in Active Exploitation Campaign	https://securityweek.com/hackers-target-zimbra-servers-in-active-exploitation-campaign
Critical Elementor Pro bug exposes WordPress sites to RCE attacks	https://bleepingcomputer.com/news/security/critical-elementor-pro-bug-exposes-wordpress-sites-to-rce-attacks
JFrog Artifactory Flaws Enable Software Supply Chain Attacks	https://infosecurity-magazine.com/news/jfrog-flaws-software-supply-chain
Isolated-vm Flaw Lets Sandboxed JavaScript Escape to Host for Potential RCE	https://thehackernews.com/2026/08/isolated-vm-flaw-lets-sandboxed.html
Critical NetScaler Flaw Can Bypass Authentication on Certain Gateway and AAA Servers	https://thehackernews.com/2026/08/critical-netscaler-flaw-can-bypass.html
Attackers Exploit Zimbra SNMP Flaw for Unauthenticated Remote Code Execution	https://thehackernews.com/2026/08/attackers-exploit-zimbra-snmp-flaw-for.html
Atlassian, Splunk Patch Dozens of Critical, High-Severity Vulnerabilities	https://securityweek.com/atlassian-splunk-patch-dozens-of-critical-high-severity-vulnerabilities
Citrix urges admins to patch new NetScaler flaws as soon as possible	https://bleepingcomputer.com/news/security/citrix-urges-admins-to-patch-new-netscaler-flaws-as-soon-as-possible
MLflow Vulnerability Exploited for Cloud Credential Theft	https://securityweek.com/mlflow-vulnerability-exploited-for-cloud-credential-theft

CISA warns of hackers exploiting critical MLflow vulnerability	https://bleepingcomputer.com/news/security/cisa-warns-of-hackers-exploiting-critical-mlflow-vulnerability
Critical Zimbra RCE flaw now actively exploited in attacks	https://bleepingcomputer.com/news/security/critical-zimbra-rce-flaw-now-actively-exploited-in-attacks
New "Zombie Card" Flaw Lets Expired Visa Cards Make Contactless Payments	https://cybersecuritynews.com/zombie-card-flaw-expired-cards
Exploitation Expected for Critical Authentication Bypass Patched in Citrix NetScaler	https://securityweek.com/exploitation-expected-for-critical-authentication-bypass-patched-in-citrix-netscaler
Critical GitLab Flaw Exploited Shortly After Disclosure	https://securityweek.com/critical-gitlab-flaw-exploited-shortly-after-disclosure
Elementor Pro Flaw Could Let Unauthenticated Attackers Upload PHP and Execute Code	https://thehackernews.com/2026/08/elementor-pro-flaw-could-let.html

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
Cisco Patches Critical Crosswork, Secure Workload Vulnerabilities	https://securityweek.com/cisco-patches-critical-crosswork-secure-workload-vulnerabilities
Oracle Releases 943 Security Patches Including Critical WebLogic Full Takeover Vulnerability	https://cybersecuritynews.com/oracle-releases-943-security-patches
943 Patches Rolled Out With Oracle's August 2026 Security Update	https://securityweek.com/943-patches-rolled-out-with-oracles-august-2026-security-update

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
Hackers Exploit TrueConf Servers to Push Malware Through Legitimate Video Conference Downloads	https://cybersecuritynews.com/hackers-exploit-trueconf-servers
China-Linked Spy Campaign Uses Five New Malware Families Against Central Asian Governments	https://cybersecuritynews.com/china-linked-spy-campaign
Hackers poison arrayref Rust crate to push infostealer malware	https://bleepingcomputer.com/news/security/hackers-poison-arrayref-rust-crate-to-push-infostealer-malware
Microsoft Defender Driver Can Be Weaponized to Disable EDR and AV From Windows Kernel	https://cybersecuritynews.com/defender-driver-can-be-weaponized

Popular Rust Packages With 244M Downloads Compromised to Run Malware	https://cybersecuritynews.com/rust-packages-malware
Hackers Use Fake CAPTCHA to Install Malware That Kills 145 Security Processes	https://cybersecuritynews.com/hackers-use-fake-captcha
Threat Actor Hacks 14,000 IP Cameras in Ukraine and Russia	https://securityweek.com/threat-actor-hacks-14000-ip-cameras-in-ukraine-and-russia
Hackers Bypass Microsoft 365 MFA and Hijack Finance Mailbox to Steal Payments	https://cybersecuritynews.com/hackers-bypass-microsoft-365-mfa
New Manic Android malware can exfiltrate data through nearby devices	https://bleepingcomputer.com/news/security/new-manic-android-malware-can-exfiltrate-data-through-nearby-devices
Def Con Attendees Targeted by Persistent Phishing Campaign	https://infosecurity-magazine.com/news/def-con-attendees-persistent
Rogue ransomware affiliate poses as recovery firm to steal payments	https://bleepingcomputer.com/news/security/rogue-ransomware-affiliate-ransom-busters-poses-as-recovery-firm
Hackers Let Microsoft 365 Users Complete MFA, Then Steal Logged-In Sessions	https://cybersecuritynews.com/microsoft-365-session-theft

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
AWS Shows How to Stop a Hijacked AI Agent From Reading Data the User Cannot Access	https://cybersecuritynews.com/aws-ai-agent-data-access

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 19/08/2026–21/08/2026 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/