

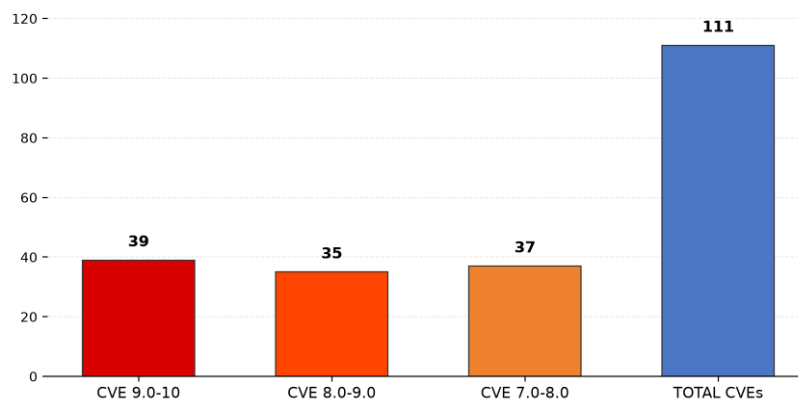


Newsletter on system vulnerabilities and cybersecurity news.

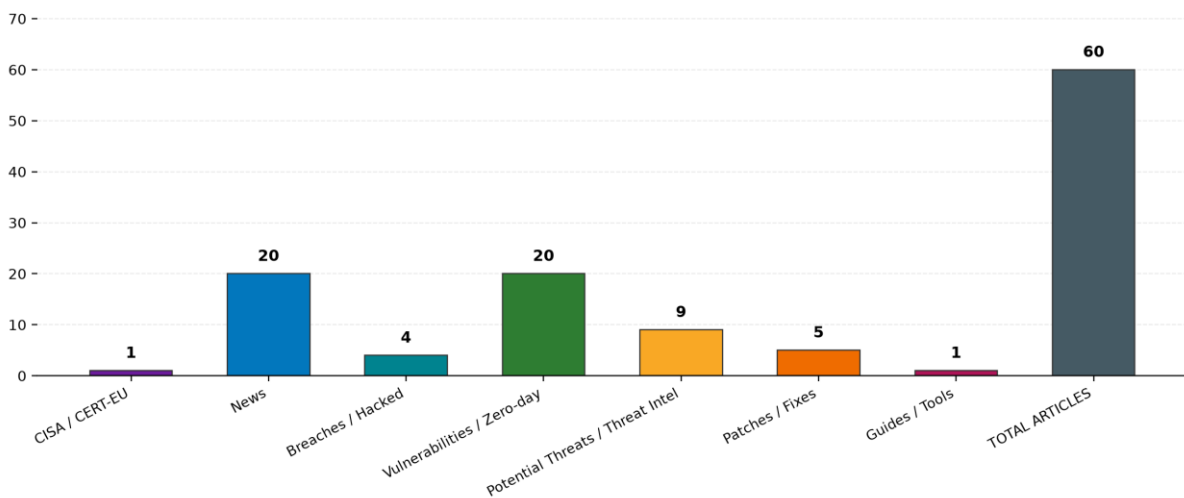
National Cyber Security Authority (NCSA)

Date: 26/08/2026 - 28/08/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories.....	13
News.....	14
Breaches / Compromised / Hacked.....	15
Vulnerabilities / Flaws / Zero-day.....	15
Patches / Updates / Fixes	16
Potential threats / Threat intelligence	17
Guides / Tools.....	17
References.....	18
Annex – Websites with vendor specific vulnerabilities	19

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-2026-77537	10,0	UniFi Protect Application	Improper Input Validation	prior to 7.2.105	https://community.ui.com/releases/Security-Advisory-Bulletin-067/fc4a3488-7c43-4628-8bab-f715e96dbfc9	none	yes	total
CVE-2026-77550	10,0	UniFi OS Server; Cloud Keys; Network Video Recorders; Enterprise Network Video Recorders; Enterprise Network Attached Storage; Dream Machines; Enterprise Firewall Core; Dream Routers; Enterprise Fortress Gateway; Cloud Gateways; Dream Wall; Express 7; Network Attached Storage; Express	Improper Neutralization of CRLF Sequences ('CRLF Injection')	prior to 5.1.37; prior to 5.1.31; prior to 5.1.32; prior to 4.0.17	https://community.ui.com/releases/Security-Advisory-Bulletin-067/fc4a3488-7c43-4628-8bab-f715e96dbfc9	none	yes	total
CVE-2026-77554	10,0	UniFi Talk Application	Improper Input Validation	prior to 5.3.2	https://community.ui.com/releases/Security-Advisory-Bulletin-067/fc4a3488-7c43-4628-8bab-f715e96dbfc9	none	yes	total
CVE-2026-77543	9,9	UniFi Access Application	Improper Input Validation	prior to 4.3.5	https://community.ui.com/releases/Security-Advisory-Bulletin-067/fc4a3488-7c43-4628-8bab-f715e96dbfc9	none	no	total
CVE-2026-59683	9,8	The OpenRGB network protocol	External Control of File Name or Path	1.0rc3 and earlier	https://bugzilla.suse.com/show_bug.cgi?id=1274007 https://gitlab.com/CalcProgrammer1/OpenRGB/-/commit/d2dd9dccc7369e78f47d01ace19af3750cd89ae66	none	yes	total
CVE-2026-65637	9,8	Apache Tomcat due to incomplete fix for CVE-2026-32990	Improper Input Validation	from 11.0.20 through 11.0.24; from 10.1.53 through 10.1.57; from 9.0.115 through 9.0.120.	https://lists.apache.org/thread/djq953z1ohsyv25bdvhfzbmsv22vqci	none	yes	total
CVE-2026-65905	9,8	Apache Tomcat's DIGEST authenticator	Authentication Bypass by Capture-replay	from 11.0.0-M1 through 11.0.24; from 10.1.0-M1 through 10.1.57; from 9.0.0-M1 through 9.0.120.; from 8.5.0 through 8.5.100; from 7.0.30 through 7.0.109.	https://lists.apache.org/thread/9v114xlpqbzrrbz5vf9f6r2q4wnxwwi http://www.openwall.com/lists/oss-security/2026/08/26/4	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-2026-74737	9,8	Linux		93a76530316a3d8cc2d 82c3deca48424fee9210 0 prior to 14fc40bf28390e0ebee6 a072457c36b82c61410 0; 93a76530316a3d8cc2d 82c3deca48424fee9210 0 prior to 1c0e35ce761131f82062 222779d857484979089 2; 93a76530316a3d8cc2d 82c3deca48424fee9210 0 prior to 9a220225efd6f58350bb b53fe70bdec08519267f ; 93a76530316a3d8cc2d 82c3deca48424fee9210 0 prior to 551688b410d3fb0dae7 73972442f268cd9446 d6; 93a76530316a3d8cc2d 82c3deca48424fee9210 0 prior to 46a8e084a159e638ac2 728e96980b65d752d65 fd; 93a76530316a3d8cc2d 82c3deca48424fee9210 0 prior to 72e4e3d7efc3b7d85f86 abbe8b94f8e45074abe 3; 93a76530316a3d8cc2d 82c3deca48424fee9210 0 prior to 914e0100df3435bd14d 09f397238e891cf9b7dc e; 93a76530316a3d8cc2d 82c3deca48424fee9210 0 prior to 36a05d2820077bb3955 acb8111e1041d391480 37; 5.7	https://git.kernel.org/stable/c/14fc40bf28390e0ebee6a072457c36b82c614100 https://git.kernel.org/stable/c/1c0e35ce761131f8206222779d8574849790892 https://git.kernel.org/stable/c/36a05d2820077bb3955acb8111e1041d39148037 https://git.kernel.org/stable/c/46a8e084a159e638ac2728e96980b65d752d65fd https://git.kernel.org/stable/c/551688b410d3fb0dae773972442f268cd9446d6 https://git.kernel.org/stable/c/72e4e3d7efc3b7d85f86abbe8b94f8e45074abe3			
CVE-2026-77552	9,8	UniFi Enterprise Audio/Video Bridge	Improper Input Validation	prior to 1.0.11	https://community.ui.com/releases/Security-Advisory-Bulletin-067/fc4a3488-7c43-4628-8bab-f715e96dbfc9	none	yes	total
CVE-2026-77557	9,8	UniFi Protect AI Key	Improper Access Control	prior to 2.2.6	https://community.ui.com/releases/Security-Advisory-Bulletin-067/fc4a3488-7c43-4628-8bab-f715e96dbfc9	none	yes	total
CVE-2026-79152	9,8	CustomTabs in Google Chrome on Android	Incorrect Authorization	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	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-2026-81700	9,8	openssl_encrypt versions	Improper Verification of Cryptographic Signature	versions before 1.4.9	https://github.com/jahives/openssl_encrypt/security/advisories/GHSA-x38r-8wf3-q9hq https://www.vulncheck.com/advisories/openssl-encrypt-before-1.4.9-qng-signature-verification-bypass	none	yes	total
CVE-2026-81702	9,8	openssl_encrypt	Insufficient Verification of Data Authenticity	before 1.4.9	https://github.com/jahives/openssl_encrypt/security/advisories/GHSA-q8p3-7h6h-qhfr https://www.vulncheck.com/advisories/openssl-encrypt-before-1.4.9-key-substitution-via-identity-load			
CVE-2026-81934	9,8	Redis	Use After Free	8.8.0	https://github.com/redis/redis/commit/6d088c335d5c3ec49a6c28486140b498e70b7834 https://github.com/v12-security/pocs/tree/main/redis/server_ssl https://raw.githubusercontent.com/redis/redis/8.10/00-RELEASENOTES https://raw.githubusercontent.com/redis/redis/8.2/00-RELEASENOTES https://raw.githubusercontent.com/redis/redis/8.4/00-RELEASENOTES https://raw.githubusercontent.com/redis/redis/8.6/00-RELEASENOTES			
CVE-2026-78900	9,6	Media in Google Chrome	Improper Input Validation	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78904	9,6	ANGLE in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78909	9,6	Views in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78935	9,6	Mobile in Google Chrome on on iOS	Use of Uninitialized Variable	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78937	9,6	Search in Google Chrome on on Android	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78939	9,6	Chromecast in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78948	9,6	WebGL in Google Chrome	Heap-based Buffer Overflow	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78951	9,6	ServiceWorker in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78964	9,6	Sync in Google Chrome on on iOS	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78985	9,6	FileSystem in Google Chrome	Use of Incorrectly-Resolved Name or Reference	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78989	9,6	ANGLE in Google Chrome on on Windows	Out-of-bounds Read	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79012	9,6	Safebrowsing in Google Chrome on on Mac	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79026	9,6	Extensions in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79052	9,6	Aura in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79064	9,6	Network in Google Chrome on on Mac	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.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-2026-79078	9,6	FedCM in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79091	9,6	Bluetooth in Google Chrome on on Mac	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79111	9,6	Dawn in Google Chrome	Improper Input Validation	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79128	9,6	Views in Google Chrome on on Mac	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79129	9,6	Sessions in Google Chrome on on An-droid	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-59682	9,1	OpenRGB	External Control of File Name or Path	through 1.0rc3.	https://bugzilla.suse.com/show_bug.cgi?id=1274000 https://gitlab.com/CalcProgrammer1/OpenRGB/-/commit/d2dd9dccc7369e78f47d01ace19af375cd89ae66	none	yes	partial
CVE-2026-65182	9,1	Apache Tomcat leads to security constraint bypass if a constraint for a longer path	Improper Access Control; In-correct Authorization	from 11.0.0-M1 through 11.0.24; from 10.1.0-M1 through 10.1.57; from 9.0.0-M1 through 9.0.120; from 8.5.0 through 8.5.100; from 7.0.0 through 7.0.109.	https://lists.apache.org/thread/0osxvzc9b49tti8l0iw9mqt0ml767m http://www.openwall.com/lists/oss-secu-ritv/2026/08/26/1	none	yes	total
CVE-2026-68525	9,1	Apache Tomcat's FORM authentica-tion process	Incorrect Authorization	from 11.0.0-M1 through 11.0.24; from 10.1.0-M1 through 10.1.57; from 9.0.0-M1 through 9.0.120.; from 8.5.0 through 8.5.100; from 7.0.0 through 7.0.109.	https://lists.apache.org/thread/x1y2lfsqzxwzc456f8954ybvqn03zhd7 http://www.openwall.com/lists/oss-secu-ritv/2026/08/26/7	none	yes	total
CVE-2026-77535	9,1	UniFi Network Application	Improper Input Validation	prior to 10.5.67	https://community.ui.com/releases/Security-Advisory-Bulletin-067/fc4a3488-7c43-4628-8bab-f715e96dbfc9	none	no	total
CVE-2026-77551	9,0	UniFi Connect Dis-play Cast Pro	Improper Access Control	prior to 1.0.111	https://community.ui.com/releases/Security-Advisory-Bulletin-067/fc4a3488-7c43-4628-8bab-f715e96dbfc9	none	no	total
CVE-2026-78891	8,8	WebRTC in Google Chrome	Heap-based Buffer Overflow	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78899	8,8	V8 in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78944	8,8	DevTools in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78990	8,8	Compositing in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79069	8,8	Tint in Google Chrome on on Mac	Improper Restriction of Oper-ations within the Bounds of a Memory Buffer	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79073	8,8	Parser in Google Chrome	Improper Check for Unusual or Exceptional Conditions	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79119	8,8	PDF in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79142	8,8	ANGLE in Google Chrome on on An-droid	Heap-based Buffer Overflow	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.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-2026-79183	8,8	Accessibility in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79195	8,8	Script in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79209	8,8	Animation in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79219	8,8	Bluetooth in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-81579	8,8	In WibuKey for Windows	Write-what-where Condition	before version 6.71	https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/AdvisoryWIBU-100031.pdf	none	no	total
CVE-2026-81581	8,8	WibuKey64	Improper Restriction of Operations within the Bounds of a Memory Buffer	up to 6.70	https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/AdvisoryWIBU-100057.pdf	none	no	total
CVE-2026-81683	8,4	openssl_encrypt (pip package openssl-encrypt)	Cleartext Storage of Sensitive Information	versions 1.4.8 and earlier	https://github.com/jahilives/openssl_encrypt/security/advisories/GHSA-r8gw-6hfi-98jw https://www.vulncheck.com/advisories/openssl-encrypt-before-1.4.9-plaintext-private-key-storage	none	no	total
CVE-2026-78911	8,3	USB in Google Chrome	Incorrect Authorization	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78934	8,3	ReadAloud in Google Chrome	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78952	8,3	Crashpad in Google Chrome on Windows	Out-of-bounds Write	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-78999	8,3	Navigation in Google Chrome	Improper Privilege Management	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79008	8,3	GPU in Google Chrome on Android	Improper Input Validation	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79071	8,3	GPU in Google Chrome	Time-of-check Time-of-use (TOCTOU) Race Condition	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79109	8,3	Printing in Google Chrome	Improper Input Validation	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79132	8,3	Input in Google Chrome on Android	Improper Input Validation	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79175	8,3	Accessibility in Google Chrome on Windows	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79218	8,3	Sandbox in Google Chrome	Incorrect Authorization	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79247	8,3	Chromoting in Google Chrome on Windows	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79256	8,3	WebView in Google Chrome on Android	Externally Controlled Reference to a Resource in Another Sphere	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.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-2026-19889	8,2	the GitLab AI Gateway component affecting all	Server-Side Request Forgery (SSRF)	from 18.9.0 to 19.0.12; 19.1 to 19.1.7; 19.2 to 19.2.2	https://gitlab.com/gitlab-org/gitlab/-/work_items/614164 https://hackerone.com/reports/3938027	poc	no	total
CVE-2026-80208	8,2	APITable	Missing Authentication for Critical Function	through 1.13.0-beta.1	https://github.com/apitable/apitable https://github.com/apitable/apitable/blob/88b24ce9f359cc434778be75d03603182882dc76/backend-server/application/src/main/java/com/apitable/internal/controller/InternalUserController.java#L149 https://github.com/apitable/apitable/issues/1812 https://www.vulncheck.com/advisories/apitable-through-1.13.0-beta.1-missing-authentication-on-the-internal-account-closure-endpoints			
CVE-2026-65183	8,1	Apache Tomcat when creating unix domain sockets	Time-of-check Time-of-use (TOCTOU) Race Condition	from 11.0.0-M1 through 11.0.24; from 10.1.0-M1 through 10.1.57; from 9.0.42 through 9.0.120.	https://lists.apache.org/thread/748o4st6d5dk6n3l7qz05vl68ga05c0 http://www.openwall.com/lists/oss-security/2026/08/26/2	none	no	total
CVE-2026-66422	8,1	Tomcat	Improper Authorization	from 11.0.0-M1 through 11.0.24; from 10.1.0-M1 through 10.1.57; from 9.0.25 through 9.0.120.; from 8.5.46 through 8.5.100; from 7.0.97 through 7.0.109.	https://lists.apache.org/thread/5plyz1b2vhqvbkn7k58nvqxhpk73 http://www.openwall.com/lists/oss-security/2026/08/26/6	none	no	partial
CVE-2026-68569	8,1	Apache Tomcat meant that in some circumstances (e	Improper Authentication	from 11.0.0-M1 through 11.0.24; from 10.1.0-M1 through 10.1.57; from 9.0.0-M1 through 9.0.120.; from 8.5.0 through 8.5.100; from 7.0.0 through 7.0.109.	https://lists.apache.org/thread/8robqa76q0osxaw0b5lcwgz0hcf9h4zc http://www.openwall.com/lists/oss-security/2026/08/26/8	none	no	total
CVE-2026-78913	8,1	Chromoting in Google Chrome	Use After Free	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79057	8,1	Start in Google Chrome on on Android	Time-of-check Time-of-use (TOCTOU) Race Condition	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-81029	8,1	OpenMetadata	URL Redirection to Untrusted Site ('Open Redirect')	prior to 2.0.0	https://github.com/open-metadata/OpenMetadata https://github.com/open-metadata/OpenMetadata/blob/1.12.1/openmetadata-service/src/main/java/org/openmetadata/service/security/saml/SamlLoginServlet.java https://github.com/open-metadata/OpenMetadata/issues/29662 https://www.vulncheck.com/advisories/openmetadata-before-2.0.0-jwt-disclosure-via-unvalidated-saml-and-oidc-redirect-uri	poc	no	total
CVE-2026-44629	7,9	Synergis Softwire	Insecure Storage of Sensitive Information		https://techdocs.genetec.com/r/en-US/Security-Updates-for-SynergisTM-Softwire-12.0/Resolved-vulnerabilities-in-Synergis-Softwire-12.0.2 https://techdocs.genetec.com/r/en-US/Security-Updates-for-SynergisTM-Softwire-12.2/Resolved-vulnerabilities-in-Synergis-Softwire-12.2.0			
CVE-2026-34674	7,8	Substance3D - Sampler	Heap-based Buffer Overflow	versions 5.1.3 and earlier	https://helpx.adobe.com/security/products/substance3d-sampler/apsb26-54.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-2026-77652	7,8	the Dia diagram editor WPG file format importer	Heap-based Buffer Overflow	0.98+git20260221-1 and earlier	https://access.redhat.com/security/cve/CVE-2026-77652 https://bugzilla.redhat.com/show_bug.cgi?id=2520884 https://gitlab.gnome.org/GNOME/dia/-/blob/master/plug-ins/wpg/wpg-import.c https://gitlab.gnome.org/GNOME/dia/-/issues/580	poc	no	total
CVE-2026-77658	7,8	the Dia diagram editor when processing Network Bus objects from Dia XML project files	Stack-based Buffer Overflow	0.98.0 and earlier	https://access.redhat.com/security/cve/CVE-2026-77658 https://bugzilla.redhat.com/show_bug.cgi?id=2520890 https://gitlab.gnome.org/GNOME/dia/-/blob/master/objects/network/bus.c https://gitlab.gnome.org/GNOME/dia/-/issues/581	poc	no	total
CVE-2026-80521	7,8	unix_del_edge()		4090fa373f0e763c43610853d2774b5979915959 prior to e3702470ced94fad74d71e2232f022d2eb752a6d; 4090fa373f0e763c43610853d2774b5979915959 prior to 594d905195024b228c962627ae5ae7c17bd582a4; 5dfd283f4651d04dbb70ceb9ae5c4a30eda3c52a; de7921631ff323369aa63a4324695ab54ea4047e; 6.1.141 prior to 6.2; 6.6.93 prior to 6.7; 6.10	https://git.kernel.org/stable/c/594d905195024b228c962627ae5ae7c17bd582a4 https://git.kernel.org/stable/c/e3702470ced94fad74d71e2232f022d2eb752a6d			
CVE-2026-80531	7,8	xrep_tempfile_create LOLLM noticed a potential UAF if the tempfile creation code fails after it set sc->tempip		84c14ee39dd388d73054181c70b3f42af7ddc238 prior to 08a20776ce33a2a52d856911e447c59424f0465a; 84c14ee39dd388d73054181c70b3f42af7ddc238 prior to cd1f876d1bc2e94f271e07c606cacd85b109108a; 84c14ee39dd388d73054181c70b3f42af7ddc238 prior to 96246a3200d32a43766152e56bc7ae2d93604d74; 84c14ee39dd388d73054181c70b3f42af7ddc238 prior to 0c88e10d12de9ca7cbed1467bb1b52310101bff8; 6.10	https://git.kernel.org/stable/c/08a20776ce33a2a52d856911e447c59424f0465a https://git.kernel.org/stable/c/0c88e10d12de9ca7cbed1467bb1b52310101bff8 https://git.kernel.org/stable/c/96246a3200d32a43766152e56bc7ae2d93604d74 https://git.kernel.org/stable/c/cd1f876d1bc2e94f271e07c606cacd85b109108a			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-81572	7,8	codemeter-runtime	Improper Link Resolution Before File Access ('Link Following')	8.40 prior to 8.41a; 9.00 prior to 9.10	https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/AdvisoryWIBU-103081.pdf https://shelltrail.com/research/local-privilege-escalation-to-system-in-wibu-systems-codemeter-application	none	no	total
CVE-2026-47879	7,7	Spring Cloud Gateway JsonToGrpcGatewayFilterFactory	Server-Side Request Forgery (SSRF)	3.1.13 and earlier	https://spring.io/security/cve-2026-47879	none	no	total
CVE-2026-75889	7,7	Alloy		1.0.0 through 1.18.1	https://grafana.com/security/security-advisories/cve-2026-75889			
CVE-2026-81576	7,7	If configured as a server, CodeMeter Runtime	Authorization Bypass Through User-Controlled Key	9.00 prior to 9.10; 8.00 prior to 8.41a; 7.00; 6.00	https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/AdvisoryWIBU-103401.pdf	none	no	partial
CVE-2026-81679	7,7	OpenRemote versions	Exposure of Sensitive Information to an Unauthorized Actor	versions before 1.28.0	https://github.com/openremote/openremote/security/advisories/GHSA-6ff4-4frc-r287 https://www.vulncheck.com/advisories/openremote-before-1.28.0-cross-realm-information-disclosure-via-notification-api			
CVE-2026-38822	7,6	In openNDS	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 11.0.0	https://github.com/openNDS/openNDS/commit/294983e859bb678ee7db06fc9f6afab0b489d8e			
CVE-2026-59284	7,6	There is no		3.1.10 and earlier	https://spring.io/security/cve-2026-59284			
CVE-2026-18983	7,5	The One User Avatar User Profile Picture plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 2.5.4	https://plugins.trac.wordpress.org/browser/one-user-avatar/trunk/includes/class-wp-user-avatar.php#L45 https://plugins.trac.wordpress.org/browser/one-user-avatar/trunk/includes/class-wp-user-avatar.php#L546 https://plugins.trac.wordpress.org/browser/one-user-avatar/trunk/includes/class-wp-user-avatar.php#L549 https://plugins.trac.wordpress.org/changeset/3659509/one-user-avatar/trunk/includes/class-wp-user-avatar.php https://plugins.trac.wordpress.org/changeset?old_path=%2Fone-user-avatar/tags/2.5.4&new_path=%2Fone-user-avatar/tags/2.5.5 https://www.wordfence.com/threat-intel/vulnerabilities/id/f413b610-839a-4a93-aec5-b6566371ccb7?source=cve			
CVE-2026-19715	7,5	The WP OAuth Server (Login with WordPress) WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 6.3.1	https://wpscan.com/vulnerability/94987bd9-7ac2-44fd-93df-52892c2a4622/	none	yes	partial
CVE-2026-36851	7,5	UnPoller	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://github.com/SyntaxSaivan/CVE-2026-36851 https://github.com/unpoller/unpoller	poc	yes	partial
CVE-2026-68763	7,5	Apache Tomcat via an allocation leak in the HTTP/2 backlog tracking when a stream	Uncontrolled Resource Consumption	from 11.0.0-M1 through 11.0.24; from 10.1.0-M1 through 10.1.57; from 9.0.39 through 9.0.120.; from 8.5.59 through 8.5.100.	https://lists.apache.org/thread/tv51tv39ppv41v04hdtkp9dp7ta02nzi http://www.openwall.com/lists/oss-security/2026/08/26/9	none	yes	partial
CVE-2026-75328	7,5	In DocSys-master	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://github.com/fang-tang7/CVE/blob/main/DocSys/DocSys%E4%BB%BB%E6%84%8F%E6%96%87%E4%B6%B6%E8%AF%BB%E5%8F%96.md	poc	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-75333	7,5	yx-image-recognition	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://github.com/fangtang7/CVE/blob/main/yx-image-recognition/PATH_TRAVERSAL_REPORT.md	poc	yes	partial
CVE-2026-75418	7,5	the built-in pre-view/development web server of Lektor		<3.3	https://github.com/TKar0/TKar0-CvePoc/tree/main/2026-CVE-POC/CVE-2026-75418 https://github.com/lektor/lektor			
CVE-2026-78137	7,5	The StoreGrowth WordPress plugin	Missing Authorization	before 2.1.2	https://wpscan.com/vulnerability/15d1a53b-c5f3-4509-9889-ddc48507df35/	none	yes	partial
CVE-2026-78915	7,5	Enterprise in Google Chrome on Windows	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79139	7,5	Media in Google Chrome on Windows	Improper Input Validation	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-79216	7,5	Blink in Google Chrome	Heap-based Buffer Overflow	prior to 152.0.7977.65	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_0256176589.html	none	no	total
CVE-2026-80347	7,5	mcp-fetch	Server-Side Request Forgery (SSRF)	1.6.3 and earlier	https://github.com/kazuph/mcp-fetch https://github.com/kazuph/mcp-fetch/issues/16 https://www.npmjs.com/package/@kazuph/mcp-fetch https://www.vulncheck.com/advisories/mcp-fetch-through-1.6.3-server-side-request-forgery-via-unstripped-ipv6-literal-brackets	poc	yes	partial
CVE-2026-81692	7,5	openssl_encrypt (pip: openssl-encrypt)	Memory Allocation with Excessive Size Value	versions 1.4.8 and earlier	https://github.com/jahilives/openssl_encrypt/security/advisories/GHSA-wr9q-p3ri-vqq7 https://www.vulncheck.com/advisories/openssl-encrypt-before-1.4.9-denial-of-service-via-streaminfo			
CVE-2026-54550	7,4	IzPack	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	5.2.6 and earlier	https://github.com/izpack/izpack/commit/4233ba38d0f1825f9cf3e0204e5261a5498e29d8 https://github.com/izpack/izpack/commit/8b7c6792c4fe85e3b1759c106aae39b904848466 https://github.com/izpack/izpack/pull/1193 https://github.com/izpack/izpack/security/advisories/GHSA-f63q-88ci-hif9	poc	no	partial
CVE-2026-18252	7,3	GitLab EE affecting all	Inclusion of Functionality from Untrusted Control Sphere	18; before 19.1.7, 19.2; before 19.2.5; before 19.3.1	https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-1-released/ https://gitlab.com/gitlab-org/gitlab/-/work_items/607342 https://hackerone.com/reports/3863650	none	no	total
CVE-2026-81690	7,3	openssl-encrypt (pip package)	Improper Link Resolution Before File Access ('Link Following')	before 1.4.9; 1.4	https://github.com/jahilives/openssl_encrypt/security/advisories/GHSA-hw7h-wqf5-6cpx https://www.vulncheck.com/advisories/verify-usb-before-1.4.9-symlink-directory-traversal-code-execution	none	no	partial
CVE-2026-13415	7,2	The CMP WordPress plugin	Improper Privilege Management	before 4.1.18	https://wpscan.com/vulnerability/f0380d89-6e49-462a-b158-9d2cc3f049ca/	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-2026-18324	7,2	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.57.0.1	https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/admin/views/custom-form/entries/content-details.php#L211 https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/build/is/shared-ui.min.js#L1 https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/library/abstracts/abstract-class-front-action.php#L127 https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/library/fields/textarea.php#L411 https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/library/modules/custom-forms/admin/admin-page-entries.php#L338 https://plugins.trac.wordpress.org/browser/forminator/tags/1.56.0/admin/views/custom-form/entries/content-details.php#L211			
CVE-2026-18978	7,2	The LiteSpeed Cache plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 7.8.1	https://plugins.trac.wordpress.org/browser/litespeed-cache/trunk/src/media.cls.php#L1317 https://plugins.trac.wordpress.org/browser/litespeed-cache/trunk/src/media.cls.php#L1358 https://plugins.trac.wordpress.org/browser/litespeed-cache/trunk/src/media.cls.php#L1405 https://plugins.trac.wordpress.org/browser/litespeed-cache/trunk/src/media.cls.php#L777 https://plugins.trac.wordpress.org/changeset/3635849/litespeed-cache/trunk/src/media.cls.php https://plugins.trac.wordpress.org/changeset?old_path=%2Flitespeed-cache/tags/7.8.1&new_path=%2Flitespeed-cache/tags/7.9			
CVE-2026-19223	7,2	The Smush WordPress plugin	Improper Control of Generation of Code ('Code Injection')	before 4.3.2	https://wpscan.com/vulnerability/77187a44-9850-4b7e-a6c2-84de660f46a3/	none	no	total
CVE-2026-76053	7,2	The TranslatePress – Translate Multilingual sites with AI Translation plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 3.3.3	https://plugins.trac.wordpress.org/browser/translatepress-multilingual/tags/3.3.1/assets/lib/simplehtmldom/simple_html_dom.php#L1549 https://plugins.trac.wordpress.org/browser/translatepress-multilingual/tags/3.3.1/assets/lib/simplehtmldom/simple_html_dom.php#L2125 https://plugins.trac.wordpress.org/browser/translatepress-multilingual/tags/3.3.1/assets/lib/simplehtmldom/simple_html_dom.php#L2220 https://plugins.trac.wordpress.org/browser/translatepress-multilingual/tags/3.3.1/assets/lib/simplehtmldom/simple_html_dom.php#L497 https://plugins.trac.wordpress.org/browser/translatepress-multilingual/tags/3.3.1/includes/class-translation-render.php#L1226 https://plugins.trac.wordpress.org/browser/translatepress-multilingual/tags/3.3.1/includes/class-translation-render.php#L664			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-77365	7,2	The Optimole – Optimize Images Convert WebP & AVIF CDN & Lazy	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 4.2.10	https://plugins.trac.wordpress.org/browser/optimole-wp/tags/4.2.10/inc/manager.php#L468 https://plugins.trac.wordpress.org/browser/optimole-wp/tags/4.2.10/inc/rest.php#L159 https://plugins.trac.wordpress.org/browser/optimole-wp/tags/4.2.10/inc/rest.php#L935 https://plugins.trac.wordpress.org/browser/optimole-wp/tags/4.2.10/inc/v2/PageProfiler/Profile.php#L189 https://plugins.trac.wordpress.org/browser/optimole-wp/tags/4.2.10/inc/v2/PageProfiler/Profile.php#L485 https://plugins.trac.wordpress.org/browser/optimole-wp/tags/4.2.7/inc/manager.php#L468			
CVE-2026-80346	7,1	StarRocks	Missing Authorization	4.0.13 and earlier	https://github.com/StarRocks/starrocks/blob/3.5.19/fe/fe-core/src/main/java/com/starrocks/alter/AlterJobMgr.java#L189 https://github.com/StarRocks/starrocks/blob/3.5.19/fe/fe-core/src/main/java/com/starrocks/sql/analyzer/AuthorizerStmtVisitor.java#L189 https://github.com/StarRocks/starrocks/issues/76566 https://www.vulncheck.com/advisories/starrocks-through-4.0.13-missing-authorization-on-drop-materialized-view-for-legacy-synchronous-materialized-views			
CVE-2026-80350	7,1	IPv4 form and a small set of IPv6 forms, but	Server-Side Request Forgery (SSRF)	prior to 12.0.7	https://github.com/OneUptime/oneuptime/blob/12.0.6/Common/Server/Utils/SSRFProtection.ts https://github.com/OneUptime/oneuptime/issues/2578 https://github.com/OneUptime/oneuptime/security/advisories/GHSA-9q3w-r349-3vww https://www.vulncheck.com/advisories/oneuptime-before-12.0.7-server-side-request-forgery-via-ipv4-mapped-ipv6-webhook-url	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 Three Known Exploited Vulnerabilities to Catalog CISA	CISA has added three new vulnerabilities to its KEV Catalog, based on evidence of active exploitation.	https://cisa.gov/news-events/alerts/2026/08/27/cisa-adds-three-known-exploited-vulnerabilities-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
Claude Code Opus 5 Auto Mode Hijacked via Prompt Injection to Execute Malicious Code	https://cybersecuritynews.com/claude-code-opus-5-auto-mode-hijacked
100+ Tech and Security Organizations Call for Global Cyber Defense Surge Against AI Attacks	https://cybersecuritynews.com/ai-cyber-defense-letter
Hackers Abuse Active Directory SPN Misconfigurations for Stealthy Kerberoasting Attacks	https://cybersecuritynews.com/active-directory-spn-misconfigurations
Nearly 700 rogue AI agents coordinated in the Hugging Face attack	https://bleepingcomputer.com/news/security/nearly-700-rogue-ai-agents-coordinated-in-the-hugging-face-attack
Chinese Routers Sold Worldwide Contain Backdoors	https://darkreading.com/vulnerabilities-threats/chinese-routers-sold-worldwide-backdoors
OpenAI Says Reward Hacking Drove AI Agents to Exploit Zero-Days and Breach Hugging Face	https://thehackernews.com/2026/08/openai-says-reward-hacking-drove-ai.html
Cybercriminals Are Selling Corporate Executives' Social Security Numbers for Just 25 Cents	https://cybersecuritynews.com/executive-social-security-numbers
Trump Order Aims to Block Foreign Backdoors in US Power Grid Gear	https://securityweek.com/trump-order-aims-to-block-foreign-backdoors-in-us-power-grid-gear
Android 17 adds ECH support to make web browsing harder to track	https://bleepingcomputer.com/news/security/android-17-adds-ech-support-to-make-web-browsing-harder-to-track
Amazon Kiro Prompt Injection Can Exfiltrate Sensitive Data Through Kiro Powers	https://thehackernews.com/2026/08/amazon-kiro-prompt-injection-can.html
Australia arrests alleged TeamPCP hackers behind supply-chain attacks	https://bleepingcomputer.com/news/security/australia-arrests-alleged-teampcp-hackers-behind-supply-chain-attacks
Manchester Airports Group Hit by Cyber Incident	https://infosecurity-magazine.com/news/manchester-airports-data-breach
Australia Arrests 2 Alleged TeamPCP Hackers	https://securityweek.com/australia-arrests-2-alleged-teampcp-hackers
Webinar: How Google Workspace breaches happen and what to do next	https://bleepingcomputer.com/news/security/webinar-how-google-workspace-breaches-happen-and-what-to-do-next
Chinese Hacker Group QTFY Uses Custom-Built Platforms to Target US Inf	https://infosecurity-magazine.com/news/chinese-qtfy-us-infrastructure-fbi
OpenAI Agents Coordinated via Makeshift Message Board Ahead of Hugging Face Hack	https://securityweek.com/openai-agents-coordinated-via-makeshift-message-board-ahead-of-hugging-face-hack
Alleged TeamPCP Hackers Charged in Australia Over Major Supply Chain Attacks	https://thehackernews.com/2026/08/alleged-teampcp-hackers-charged-in.html
Okta Shares Surge on Strong Earnings, Growing Demand for AI Identity Security	https://securityweek.com/okta-shares-surge-on-strong-earnings-growing-demand-for-ai-identity-security
Russian Hackers Phish EU Officials Over Messaging Apps	https://darkreading.com/cyberattacks-data-breaches/russian-hackers-phish-eu-officials-messaging-apps
CISO Conversations: Chris Wheeler – Trust Is the Job, From the Navy to the C-Suite	https://securityweek.com/ciso-conversations-chris-wheeler-trust-is-the-job-from-the-navy-to-the-c-suite

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
Hackers Steal Data of 8.7 Million Customers in Cyberattack on Three UK Airports	https://cybersecuritynews.com/hackers-steal-data-of-three-uk-airports
Manchester Airports Group says hackers stole travelers' data	https://bleepingcomputer.com/news/security/manchester-airports-group-says-hackers-stole-travelers-data
Carhartt data breach exposes information of 12.9 million accounts	https://bleepingcomputer.com/news/security/carhartt-data-breach-exposes-information-of-129-million-accounts
CISA Red Team Compromised Two Critical Infrastructure Orgs, One Detected Nothing	https://thehackernews.com/2026/08/cisa-red-team-compromised-two-critical.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
CISA Warns of Linux Kernel Privilege Escalation Vulnerability Exploited in Attacks	https://cybersecuritynews.com/linux-kernel-privilege-escalation-vulnerability-exploited
Critical cPanel Vulnerability Allows Attackers to Take Full Server Control	https://cybersecuritynews.com/critical-cpanel-vulnerability
PaperCut NG/MF Vulnerability Actively Exploited in Attack - All Versions Impacted	https://cybersecuritynews.com/papercut-ng-mf-vulnerability-actively-exploited
CISA Warns of Citrix NetScaler ADC and Gateway Vulnerability Exploited in Attacks	https://cybersecuritynews.com/citrix-netscaler-adc-and-gateway-vulnerability-exploited
PaperCut warns of NG, MF flaw exploited in zero-day attacks	https://bleepingcomputer.com/news/security/papercut-warns-of-ng-mf-flaw-exploited-in-zero-day-attacks
CISA Warns of Six Exploited Flaws in Microsoft, Linux and Citrix	https://infosecurity-magazine.com/news/cisa-kev-microsoft-citrix
Veeam Backup & Replication Flaw Exposes Guest OS Credentials in Cleartext Logs	https://cybersecuritynews.com/veeam-backup-replication-flaw-exposes
CISA orders feds to patch Citrix NetScaler RCE flaw by Saturday	https://bleepingcomputer.com/news/security/cisa-hackers-now-exploiting-citrix-netscaler-rce-flaw-in-attacks
New Apache Log4j2 Flaw Lets Attackers Bypass Security Checks and Execute Remote Code	https://cybersecuritynews.com/new-apache-log4j2-flaw
CISA Adds Six Exploited Flaws to KEV, Including NetScaler, Linux, and SQL Server Bugs	https://thehackernews.com/2026/08/cisa-adds-six-exploited-flaws-to-kev.html
Recent Citrix NetScaler Vulnerability Exploited in the Wild	https://securityweek.com/recent-citrix-netscaler-vulnerability-exploited-in-the-wild
WatchGuard Agent for Windows Vulnerability Allows Code Execution with Elevated Privileges	https://cybersecuritynews.com/watchguard-agent-for-windows-vulnerability

Σύντομη περιγραφή / Τίτλος	URL
Adobe Campaign Classic Vulnerabilities Enable Arbitrary Code Execution	https://cybersecuritynews.com/adobe-campaign-classic-code-execution
Apache Tomcat Vulnerabilities Let Attackers Bypass Security Controls and Crash Servers	https://cybersecuritynews.com/apache-tomcat-vulnerabilities-crash-servers
Critical Avada WordPress theme flaw enables zero-click RCE	https://bleepingcomputer.com/news/security/critical-avada-wordpress-theme-flaw-enables-zero-click-rce
21 Critical Ubiquiti UniFi Flaws Enable Authentication Bypass, Command Injection and Privilege Escalation	https://cybersecuritynews.com/21-critical-ubiquiti-unifi-flaws
Critical Next.js Vulnerabilities Enables Remote Code Execution Attacks	https://cybersecuritynews.com/next-js-vulnerabilities
Adobe and Nvidia Patch Dozens of Vulnerabilities	https://securityweek.com/adobe-and-nvidia-patch-dozens-of-vulnerabilities
Google Chrome 152 Released With 327 Security Fixes, Including 10 Critical Vulnerabilities	https://cybersecuritynews.com/chrome-152-released-with-327-security-fixes
Critical Gitea RCE Actively Exploited as Reported Attack Drops Miner-Like Payload	https://thehackernews.com/2026/08/critical-gitea-rce-actively-exploited.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
Next.js Patches Critical AVIF and Windows Flaws Enabling Unauthenticated RCE	https://thehackernews.com/2026/08/nextjs-patches-critical-avif-and.html
Microsoft rolls out fix for Windows 11 crashes, gaming issues	https://bleepingcomputer.com/news/microsoft/microsoft-rolls-out-fix-for-windows-11-crashes-gaming-issues
Ubiquiti patches three max severity security vulnerabilities	https://bleepingcomputer.com/news/security/ubiquiti-patches-three-max-severity-security-vulnerabilities
Unpatched Kaltura mwEmbed Flaws Could Let Remote Attackers Read Files and Run Code	https://thehackernews.com/2026/08/unpatched-kaltura-mwembed-flaws-could.html
Chrome 152 Patches Over 300 Vulnerabilities	https://securityweek.com/chrome-152-patches-over-300-vulnerabilities

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
Threat Actors Abuse Cursor Agent AI to Assist Ransomware Operations	https://infosecurity-magazine.com/news/abuse-cursor-agent-ransomware
Dark Caracal Hackers Use Ethereum Blockchain to Keep New Malware Connected After C2 Disruption	https://cybersecuritynews.com/dark-caracal-hackers
ThreatsDay: 296K IoT Botnet, 100+ Water Systems Targeted, SharePoint RCE Chain + 27 New Stories	https://thehackernews.com/2026/08/threatsday-296k-iot-botnet-100-water.html
Spark RAT Targets Cambodia, Abuses Vulnerable OPSWAT Driver to Disable Security Tools	https://thehackernews.com/2026/08/spark-rat-targets-cambodia-abuses.html
New Windows Backdoor Hides Inside ESET Agent and Wakes Up With a Secret Network Packet	https://cybersecuritynews.com/new-windows-backdoor
Android Malware Hijacks Update System for Car Head Units	https://darkreading.com/cyberattacks-data-breaches/android-malware-hijacks-update-system-car-head-units
Tortoiseshell Expands Toolset With New Backdoor, SSH Tunnel	https://infosecurity-magazine.com/news/tortoiseshell-new-backdoor-ssh
Iran-Linked Hackers Expand Attacks With New Backdoor and Reverse SSH Tunnels	https://cybersecuritynews.com/iran-linked-hackers
Mirage2FA Phishing Kit Bypasses MFA to Hijack Microsoft 365 Sessions, Targeting 3,500+ Organizations	https://cybersecuritynews.com/mirage2fa-phishing-kit-bypasses-mfa-to-hijack-microsoft-365-sessions-targeting-3500-organizations

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
Learn How to Build Security Operations Ready for AI-Powered Attacks	https://thehackernews.com/2026/08/learn-how-to-build-security-operations.html

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 26/08/2026–28/08/2026 και η επιλογή τους έγινε με βάση το πόσο διαδεδομένα είναι τα προϊόντα-υπηρεσίες.

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/