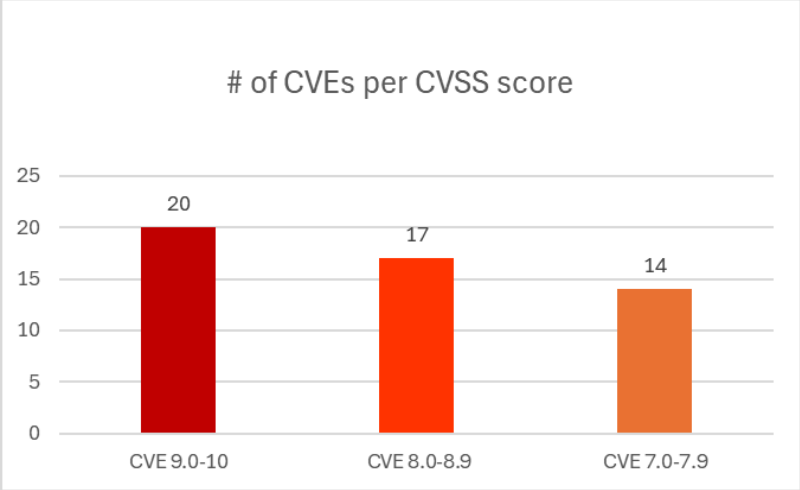
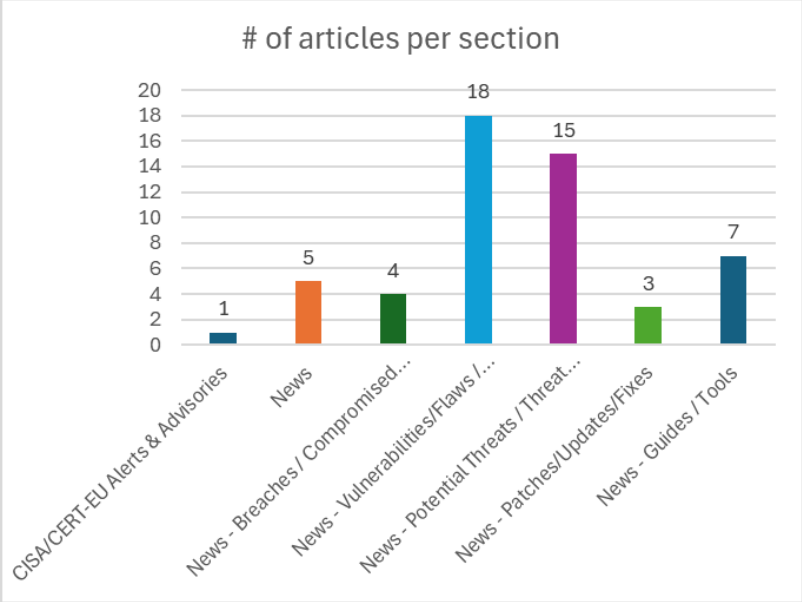
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 01/07/2026 - 03/07/2026





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 της ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

URL ευπάθειας (NIST NVD)	CVSS v3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-56004	10,0	SUSE	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	A shellcode injection in the mercurial handler of the obs tar_scm source service before version 0.12.4	https://github.com/openSUSE/obs-service-tar_scm/pull/552/changes/bcf29d318c671c45fe87dd9f995a4a0c78ecedd7
https://nvd.nist.gov/vuln/detail/CVE-2026-44935	9,9	Helm Deployer of SUSE Rancher Fleet	Improper Validation of Specified Type of Input	Helm Deployer of SUSE Rancher Fleet 0.15 before 0.15.2, 0.14 before 0.14.6, 0.13 before 0.13.11 and 0.12 before 0.12.15	https://github.com/rancher/fleet/security/advisories/GHSA-xr65-5cpm-g36x
https://nvd.nist.gov/vuln/detail/CVE-2026-45499	9,9	Azure OpenAI	Server-Side Request Forgery (SSRF)	Azure OpenAI	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45499
https://nvd.nist.gov/vuln/detail/CVE-2026-57100	9,9	Microsoft Entra Provisioning Service (SyncFabric)	Server-Side Request Forgery (SSRF)	Microsoft Entra Provisioning Service (SyncFabric)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-57100
https://nvd.nist.gov/vuln/detail/CVE-2026-24270	9,8	NVIDIA AIStore framework	Authentication Bypass by Spoofing	NVIDIA AIStore framework	https://github.com/NVIDIA/product-security/tree/main/2026/5849 https://nvd.nist.gov/vuln/detail/CVE-2026-24270 https://www.cve.org/CVERecord?id=CVE-2026-24270
https://nvd.nist.gov/vuln/detail/CVE-2026-4767	9,8	TR7 Cyber Defense Inc	Missing Authentication for Critical Function	This issue affects WAF-ASP: from v1.0.324.900 before v1.4.0.117	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-0487
https://nvd.nist.gov/vuln/detail/CVE-2026-52186	9,8	UTT	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	SQL Injection vulnerability in UTT nv518G nv518GV3v3.2.7-210919-161313	https://github.com/akuma-QAQ/CVEreport/blob/main/518G/FUN_00463bbc/README.md https://utt.com.cn/downloadcenter.php?filetyp-eid=3&model=518G&lang=zhcn
https://nvd.nist.gov/vuln/detail/CVE-2026-58453	9,8	JAIOTlink C492A-W6 Wi-Fi IP cameras	Use of Default Credentials	JAIOTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411	https://github.com/rwprimitives/jaiotlink-c492a-wifi-camera/blob/main/writeups/02-default-http-credentials.md https://www.amazon.com/stores/JAIOTlink/page/3B00DC41-70C3-4BAA-925C-3D222C2633D5?lp_asin=B0GX1BNZ78&ref_=ast_bln&store_ref=bl_ast_dp_brandlogo_sto https://www.vulncheck.com/advisories/jaiotlink-c492a-w6-hard-coded-credentials-via-anyka-ipc
https://nvd.nist.gov/vuln/detail/CVE-2026-58457	9,8	Shenzhen Aitemi M300 Wi-Fi Repeater	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT02)	https://github.com/IEATASICS/m300-repeater-bugs# https://www.aliexpress.us/item/3256806767641280.html https://www.vulncheck.com/advisories/shenzhen-aitemi-m300-mt02-unauthenticated-os-command-injection-via-protocol-csp

https://nvd.nist.gov/vuln/detail/CVE-2026-7840	9,8	UltraVNC repeater	Out-of-bounds Write	UltraVNC repeater through 1.8.2.2	https://github.com/ultravnc/UltraVNC https://uvnc.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-14405	9,6	Google Chrome	Use of Uninitialized Variable	Uninitialized Use in V8 in Google Chrome prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/513376037
https://nvd.nist.gov/vuln/detail/CVE-2026-14419	9,6	Google Chrome	Use After Free	Use after free in Skia in Google Chrome prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/516981393
https://nvd.nist.gov/vuln/detail/CVE-2026-14423	9,6	Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	Type Confusion in Tint in Google Chrome prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/517522769
https://nvd.nist.gov/vuln/detail/CVE-2026-14424	9,6	Google Chrome	Use After Free	Use after free in Dawn in Google Chrome on Mac prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/517692772
https://nvd.nist.gov/vuln/detail/CVE-2026-14425	9,6	Google Chrome	Use After Free	Use after free in ANGLE in Google Chrome prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/517935753
https://nvd.nist.gov/vuln/detail/CVE-2026-52830	9,4	Telegram MCP Server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to 0.19.1	https://github.com/advisories/GHSA-rxw2-pc8j-vxwm https://web.archive.org/web/20250926152207/https://github.com/leshchenko1979/fast-mcp-telegram
https://nvd.nist.gov/vuln/detail/CVE-2026-41106	9,3	M365 Copilot	URL Redirection to Untrusted Site ('Open Redirect')	M365 Copilot	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41106
https://nvd.nist.gov/vuln/detail/CVE-2025-23350	9,0	NVIDIA ConnectX and BlueField	Out-of-bounds Write	NVIDIA ConnectX and BlueField	https://github.com/NVIDIA/product-security/tree/main/2026/5699 https://nvd.nist.gov/vuln/detail/CVE-2025-23350 https://www.cve.org/CVERecord?id=CVE-2025-23350
https://nvd.nist.gov/vuln/detail/CVE-2025-23351	9,0	NVIDIA ConnectX and BlueField	Out-of-bounds Write	NVIDIA ConnectX and BlueField	https://github.com/NVIDIA/product-security/tree/main/2026/5699 https://nvd.nist.gov/vuln/detail/CVE-2025-23351 https://www.cve.org/CVERecord?id=CVE-2025-23351
https://nvd.nist.gov/vuln/detail/CVE-2026-55116	9,0	UniFi OS	Improper Access Control	-	https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc
https://nvd.nist.gov/vuln/detail/CVE-2026-14415	8,8	V8 in Google Chrome	Heap-based Buffer Overflow	V8 in Google Chrome prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/515086856
https://nvd.nist.gov/vuln/detail/CVE-2026-14430	8,8	V8 in Google Chrome	Integer Overflow or Wraparound	V8 in Google Chrome prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/522126182
https://nvd.nist.gov/vuln/detail/CVE-2026-14431	8,8	V8 in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	V8 in Google Chrome prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/523884658
https://nvd.nist.gov/vuln/detail/CVE-2026-14432	8,8	V8 in Google Chrome	Use After Free	V8 in Google Chrome prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/524290062
https://nvd.nist.gov/vuln/detail/CVE-2026-54998	8,8	Microsoft Exchange Online	Incorrect Authorization	Microsoft Exchange Online	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54998

https://nvd.nist.gov/vuln/detail/CVE-2026-56841	8,8	UniFi Protect	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	UniFi Protect Application	https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc
https://nvd.nist.gov/vuln/detail/CVE-2026-57766	8,8	WPIDE – File Manager & Code Editor	Cross-Site Request Forgery (CSRF)	WPIDE – File Manager & Code Editor <= 3.5.6 versions.	https://patchstack.com/database/wordpress/plugin/wpide/vulnerability/wordpress-wpide-file-manager-code-editor-plugin-3-5-6-cross-site-request-forgery-csrf-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-58452	8,8	JAIOTlink	Improper Control of Generation of Code ('Code Injection')	JAIOTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411	https://github.com/rwprimitives/jaiotlink-c492a-wifi-camera/blob/main/writeups/01-setmac-command-injection.md https://www.amazon.com/stores/JAIOTlink/page/3B00DC41-70C3-4BAA-925C-3D222C2633D5?lp_asin=B0GX1BNZ78&ref_=ast_bln&store_ref=bl_ast_dp_brandlogo_sto https://www.vulncheck.com/advisories/jaiotlink-c492a-w6-os-command-injection-via-setmac-endpoint
https://nvd.nist.gov/vuln/detail/CVE-2026-7838	8,8	UltraVNC	Integer Overflow or Wraparound	UltraVNC viewer through 1.8.2.2	https://github.com/ultravnc/UltraVNC https://uvnc.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-24260	8,5	NVIDIA Container Toolkit for Linux	Time-of-check Time-of-use (TOCTOU) Race Condition	NVIDIA Container Toolkit for Linux	https://github.com/NVIDIA/product-security/tree/main/2026/5850 https://nvd.nist.gov/vuln/detail/CVE-2026-24260 https://www.cve.org/CVERecord?id=CVE-2026-24260
https://nvd.nist.gov/vuln/detail/CVE-2026-14429	8,3	Skia in Google Chrome	Improper Input Validation	Skia in Google Chrome prior to 150.0.7871.46	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0175352312.html https://issues.chromium.org/issues/520571816
https://nvd.nist.gov/vuln/detail/CVE-2026-50521	8,3	Microsoft Edge (Chromium-based)	Use After Free	Microsoft Edge (Chromium-based)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50521
https://nvd.nist.gov/vuln/detail/CVE-2026-55118	8,3	UniFi Network	Improper Access Control	UniFi Network	https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc
https://nvd.nist.gov/vuln/detail/CVE-2026-57278	8,3	GeoWebPlayer	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	GeoWebPlayer	https://talosintelligence.com/vulnerability_reports/TALOS-2026-2375
https://nvd.nist.gov/vuln/detail/CVE-2026-14336	8,2	Jenkins tokens	Server-Side Request Forgery (SSRF)	Jenkins tokens	https://gitlab.eclipse.org/security/cve-assignment/-/work_items/154
https://nvd.nist.gov/vuln/detail/CVE-2025-58902	8,1	Lighthouse	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusio	Lighthouse <= 1.2.12 versions.	https://patchstack.com/database/wordpress/theme/lighthouseschool/vulnerability/wordpress-lighthouse-theme-1-2-12-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-55119	8,1	UniFi Talk	Improper Access Control	UniFi Talk	https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc
https://nvd.nist.gov/vuln/detail/CVE-2026-24251	7,8	NVIDIA Megatron Bridge for Linux	Deserialization of Untrusted Data	NVIDIA Megatron Bridge for Linux	https://github.com/NVIDIA/product-security/tree/main/2026/5841 https://nvd.nist.gov/vuln/detail/CVE-2026-24251 https://www.cve.org/CVERecord?id=CVE-2026-24251
https://nvd.nist.gov/vuln/detail/CVE-2026-20191	7,5	Cisco Catalyst Center	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Cisco Catalyst Center	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catc-file-read-wLH2vf8X

https://nvd.nist.gov/vuln/detail/CVE-2026-24264	7,5	NVIDIA Triton Inference Server for Linux	Improper Handling of Highly Compressed Data (Data Amplification)	NVIDIA Triton Inference Server for Linux	https://github.com/NVIDIA/product-security/tree/main/2026/5848 https://nvd.nist.gov/vuln/detail/CVE-2026-24264 https://www.cve.org/CVERecord?id=CVE-2026-24264
https://nvd.nist.gov/vuln/detail/CVE-2026-52190	7,5	UTT	Stack-based Buffer Overflow	UTT nv518G nv518GV3v3.2.7-210919-161313	https://github.com/akuma-QAQ/CVEreport/tree/main/518G/FUN_00448384 https://utt.com.cn/downloadcenter.php?filetypeid=3&model=518G&lang=zhcn
https://nvd.nist.gov/vuln/detail/CVE-2026-56842	7,5	UniFi	Incorrect Authorization	UniFi Network Application	https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc
https://nvd.nist.gov/vuln/detail/CVE-2026-58454	7,5	JAIOTlink	Improper Control of Generation of Code ('Code Injection')	JAIOTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411	https://github.com/rwprimitives/jaiotlink-c492a-wifi-camera/blob/main/writeups/03-anyka-config-execution-trigger.md https://www.amazon.com/stores/JAIOTlink/page/3B00DC41-70C3-4BAA-925C-3D222C2633D5?lp_asin=B0GX1BNZ78&ref_=ast_bln&store_ref=bl_ast_dp_brandlogo_sto https://www.vulncheck.com/advisories/jaiotlink-c492a-w6-rce-via-anyka-config-endpoint
https://nvd.nist.gov/vuln/detail/CVE-2026-58467	7,5	Cockpit CMS	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Cockpit CMS before release 364	https://github.com/cockpit-project/cockpit/releases/tag/364 https://github.com/geo-chen/oss/blob/main/cockpit.md https://www.vulncheck.com/advisories/cockpit-cms-364-path-traversal-local-file-inclusion-via-index-php
https://nvd.nist.gov/vuln/detail/CVE-2026-9563	7,5	Maven Central	Uncontrolled Resource Consumption	Maven Central before version 1.1.8	https://github.com/eclipse-ee4j/parsson/commit/134e8d101aa74c8b9302d0cb62f6ccb4912a9d0c https://github.com/eclipse-ee4j/parsson/pull/169 https://github.com/eclipse-ee4j/parsson/tree/1.1.8 https://gitlab.eclipse.org/security/vulnerability-reports/-/work_items/444 https://repo.maven.apache.org/maven2/org/eclipse/parsson/parsson/1.1.8/
https://nvd.nist.gov/vuln/detail/CVE-2026-41121	7,3	Dell Device Management Agent	Improper Link Resolution Before File Access ('Link Following')	Dell Device Management Agent, versions prior to DDMA 26.05	https://www.dell.com/support/kbdoc/en-us/000473690/dsa-2026-258
https://nvd.nist.gov/vuln/detail/CVE-2026-27404	7,1	LMS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	LMS <= 9.7 versions.	https://patchstack.com/database/wordpress/theme/lms/vulnerability/wordpress-lms-theme-9-7-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-55153	7,1	Java library	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	mchange-commons-java prior to version 0.6.0	https://github.com/swaldman/mchange-commons-java/security/advisories/GHSA-h84g-69h7-mw6v
https://nvd.nist.gov/vuln/detail/CVE-2026-57362	7,1	ChatBot	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	ChatBot <= 8.3.2 versions.	https://patchstack.com/database/wordpress/plugin/chatbot/vulnerability/wordpress-chatbot-plugin-8-3-2-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/v uln/detail/CVE-2026-57426	7,1	Modula - PRO	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Modula - PRO <= 2.10.8 versions.	https://patchstack.com/database/wordpress/plugin/modula/vulnerability/wordpress-modula-pro-plugin-2-10-8-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-57670	7,1	Google Maps CP	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Google Maps CP <= 1.2.5 versions.	https://patchstack.com/database/wordpress/plugin/codepeople-post-map/vulnerability/wordpress-google-maps-cp-plugin-1-2-5-cross-site-scripting-xss-vulnerability?_s_id=cve

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	▪ CVE-2026-45659 Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2026/07/01/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
Google Dismantles NetNut Residential Proxy That Hacked 2 Million Home Devices	https://cybersecuritynews.com/google-dismantles-netnut-residential-proxy/
Opera Blocks Clipboard Attacks, Including ClickFix, With New Paste Protect Feature	https://cybersecuritynews.com/opera-paste-protect-feature/
Critical Flaws Double as Elevation of Privilege Dominates the Cyber Threats – Analysis of Microsoft Vulnerabilities Report 2026	https://cybersecuritynews.com/microsoft-vulnerabilities-report-2026/
FortiBleed Password Stealing Attack Linked to INC and Lynx Ransomware Operations	https://cybersecuritynews.com/fortibleed-password-stealing-attack/
WhatsApp Username Reservations Go Live – What Are the Security Concerns for 2 Billion Users	https://cybersecuritynews.com/whatsapp-username-reservations-go-live/

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
Former MEP Investigating Spyware Abuses Has Phone Hacked With Pegasus	https://cybersecuritynews.com/mep-investigating-spyware-hacked-pegasus/
DHS Confirms Breach of Information-Sharing Network Platform HSIN	https://cybersecuritynews.com/dhs-confirms-breach-of-hsin/
Medtronic Confirms Data Breach – Hackers Gained Access to Corporate IT Systems	https://cybersecuritynews.com/medtronic-confirms-data-breach/
Massive Password Stealing Attack Targeting Microsoft 365 Users With 81 Million Login Attempts	https://cybersecuritynews.com/microsofts-azure-password-spray-attack/

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
Multiple WatchGuard Firebox OS Vulnerabilities Enable Arbitrary Code Execution Attacks	https://cybersecuritynews.com/watchguard-firebox-os-vulnerabilities/
Microsoft Exchange SSRF Vulnerability Details Released Along With Public PoC Exploit	https://cybersecuritynews.com/exchange-ssrf-poc-exploit-released/
Claude Cowork's Sandbox Vulnerability Allows Attackers to Run Arbitrary Commands as Root	https://cybersecuritynews.com/claude-coworks-sandbox-vulnerability/
CitrixBleed Vulnerability Exploited by Hackers Within 24 Hours of Public Disclosure	https://cybersecuritynews.com/citrixbleed-vulnerability-exploited/
ChatGPT File Download Flow Vulnerability Could Be Abused to Access System Files	https://cybersecuritynews.com/chatgpt-file-download-flow-vulnerability/
900+ Oracle E-Business instances Exposed Online Amid Active Vulnerability Exploitation	https://cybersecuritynews.com/900-oracle-e-business-instances-exposed/
Microsoft Outlook Bug Removes Copilot Button For Windows Users	https://cybersecuritynews.com/outlook-bug-removes-copilot-button/
Cisco Catalyst Center Vulnerability Allows Remote Attackers to Read Arbitrary Files	https://cybersecuritynews.com/cisco-catalyst-center-vulnerability-attackers/
Critical JetBrains Vulnerabilities Enable Authentication Bypass and Code Execution Attacks	https://cybersecuritynews.com/jetbrains-vulnerabilities/
CISA Warns of Microsoft SharePoint Server Code Execution Vulnerability Exploited in Attacks	https://cybersecuritynews.com/sharepoint-server-code-execution-vulnerability-exploited/
CISA Warns of SimpleHelp Authentication Bypass Vulnerability Exploited in Attacks	https://cybersecuritynews.com/simplehelp-auth-vulnerability-exploited/

Critical Cursor IDE RCE Vulnerabilities Enable Prompt Injection in Zero-Click	https://cybersecuritynews.com/cursor-ide-rce-vulnerabilities/
Apple 'Hide My Email' Vulnerability Exposes Users' Real Email Addresses	https://cybersecuritynews.com/apple-hide-my-email-vulnerability/
Multiple Fluentd Vulnerabilities Let Attackers Execution Arbitrary Code Remotely	https://cybersecuritynews.com/fluentd-vulnerabilities/
Critical Multiple Adobe ColdFusion Vulnerabilities Enables Arbitrary Code Execution Attacks	https://cybersecuritynews.com/multiple-adobe-coldfusion-vulnerabilities/
Anthropic's Buffa Rust Library 0-Day Vulnerability Enables DoS Attack	https://cybersecuritynews.com/anthropics-buffa-rust-library-0-day-vulnerability-enables-dos-attack/
Multiple Citrix NetScaler ADC and Gateway Vulnerabilities Enables DoS and Memory Overflow Attacks	https://cybersecuritynews.com/citrix-netscaler-vulnerabilities/
Multiple Apache Tomcat Vulnerabilities Allow Attackers to Bypass Authentication	https://cybersecuritynews.com/multiple-apache-tomcat-vulnerabilities/

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
WinRAR 7.23 Fixes Heap Overflow Vulnerability that Leads to Application Crashes	https://cybersecuritynews.com/winrar-7-23-fixes-heap-overflow-vulnerability/
Chrome Update Patches 382 Vulnerabilities Including 15 Critical One's that Enables Code Execution Attacks	https://cybersecuritynews.com/chrome-update-fixes-382-vulnerabilities/
Microsoft Teams' New Feature Blocks Bots from Joining Meetings	https://cybersecuritynews.com/microsoft-teams-bot-protection/

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συν-θήκες. Περι-λαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
North Korea-Linked Hackers Hide JavaScript Loaders in Open Source Repositories	https://cybersecuritynews.com/north-korea-linked-hackers-hide-javascript-loaders/
AsyncRAT Campaign Uses DLL Sideloading and ScreenConnect for Stealthy Remote Access	https://cybersecuritynews.com/asyncrat-campaign-uses-dll-sideloading/
Microsoft 365 Phishing Panel Uses OAuth Device Code Flow to Capture Tokens and Persist Access	https://cybersecuritynews.com/microsoft-365-phishing-panel-uses-oauth-device-code-flow/
AsyncRAT Campaign Abuses TryCloudflare Tunnels and Python Scripts for Malware Delivery	https://cybersecuritynews.com/asyncrat-campaign-abuses-trycloudflare-tunnels/
Hackers Use Fake VLC Executable and Malicious libvlc.dll to Deploy ValleyRAT	https://cybersecuritynews.com/hackers-use-fake-vlc-executable/
Agentic Ransomware JADEPUFFER Uses Base64 Python Payloads to Harvest Cloud and API Keys	https://cybersecuritynews.com/agentic-ransomware-jadepuffer-uses-base64-python-payloads/
Hackers Use Mapbox Dead-Drop C2 and Python RAT to Target Vulnerability Re-searchers	https://cybersecuritynews.com/hackers-use-mapbox-dead-drop-c2/
Hackers Disable Defender, Sysmon, and WAF Before Dumping Credentials With Mimikatz	https://cybersecuritynews.com/hackers-disable-defender-sysmon/
Browser-Only Ransomware Abuses Chrome File System Access API to Encrypt An-droid Photos	https://cybersecuritynews.com/browser-only-ransomware-abuses-chrome-file-system-access-api/
Multiple ClamAV Vulnerabilities Allow Remote Attacker to Cause a DoS Condition	https://cybersecuritynews.com/multiple-clamav-vulnerabilities/
Indian Govt Halts Meta’s WhatsApp Usernames Rollout Over Fraud Concerns	https://cybersecuritynews.com/indian-govt-whatsapp-usernames/
A Weaponized Google Ad Install Malicious Claude Code to Hijack Entire macOS	https://cybersecuritynews.com/a-weaponized-google-ad-install-malicious-claude-code-to-hijack-entire-macos/
Attackers Weaponizing Trusted Windows Drivers to Kill AV and EDR Processes	https://cybersecuritynews.com/windows-drivers-to-kill-av-and-edr/
Anthropic’s Claude Code Reportedly Uses Hidden Code to Detect Chinese Users	https://cybersecuritynews.com/anthropic-claude-hidden-code/
Hackers Use SystemBC Malware to Hide C2 Traffic and Maintain Persistent Access	https://cybersecuritynews.com/hackers-use-systembc-malware-to-hide-c2-traffic/

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
Anthropic Details Claude Fable 5 Cybersecurity Safeguards and Jailbreak Framework	https://cybersecuritynews.com/anthropic-claude-fable-5-cybersecurity/
The Business Cost of Alert Fatigue: How to Reduce Delays, Escalations for Your SOC as 70% Alerts are Un-investigated	https://cybersecuritynews.com/the-business-cost-of-alert-fatigue/
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/
CISA Releases Best Security Practices Guide for Hardening Microsoft Exchange Server	https://cybersecuritynews.com/microsoft-exchange-server-hardening-guide/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-management-tools/
NETREAPER Offensive Security Toolkit That Wraps 70+ Penetration Testing Tools	https://cybersecuritynews.com/netreaper-offensive-security-toolkit/
GitLab Security Best Practices Cheat Sheet	https://thehackernews.uk/gitlab-security-tips

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 CVSSv3 score >= 7.0 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/