

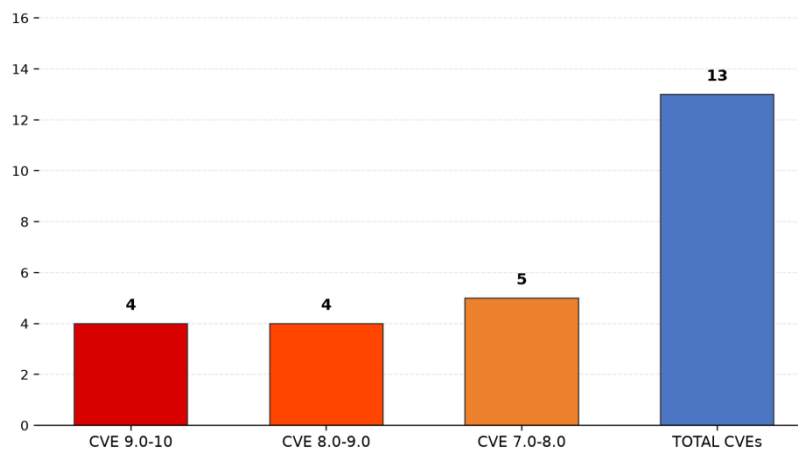


Newsletter on system vulnerabilities and
cybersecurity news.

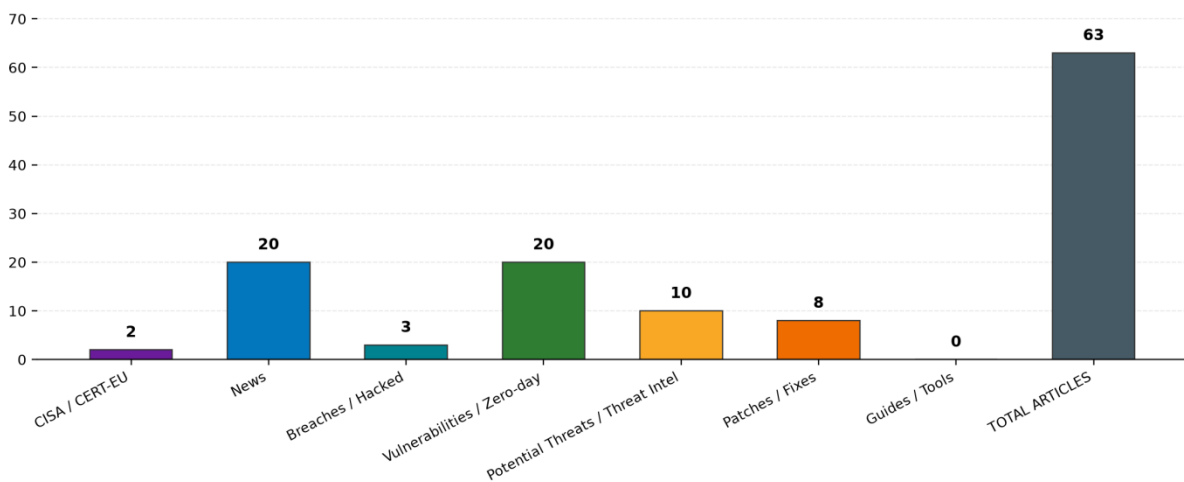
National Cyber Security Authority (NCSA)

Date: 07/10/2026 - 09/10/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories.....	4
News.....	5
Breaches / Compromised / Hacked.....	6
Vulnerabilities / Flaws / Zero-day.....	6
Patches / Updates / Fixes	7
Potential threats / Threat intelligence	8
Guides / Tools.....	8
References.....	9
Annex – Websites with vendor specific vulnerabilities	10

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-2026-104334	9,8	IBM Langflow OSS	Improper Control of Generation of Code ('Code Injection')	1.0.0 through 1.12.2	https://www.ibm.com/support/pages/node/7290694	none	yes	total
CVE-2026-78401	9,8	IBM Security Verify Access; Verify Identity Access	Deserialization of Untrusted Data	10.0 through 10.0.9.2; 11.0 through 11.0.3	https://www.ibm.com/support/pages/node/7291628	none	yes	total
CVE-2026-82335	9,8	IBM Guardium Data Protection	Improper Restriction of Operations within the Bounds of a Memory Buffer; Out-of-bounds Write	12.0; 12.1; 12.2	https://www.ibm.com/support/pages/node/7291674	none	no	total
CVE-2026-107845	9,3	Contao	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'); Improper Encoding or Escaping of Output	>= 4.0.0, < 5.3.50; >= 5.4.0-RC1, < 5.7.12	https://github.com/contao/contao/commit/22505d5f79bc1a7f52e2c8a5fdd6007e1f0408a https://github.com/contao/contao/releases/tag/5.3.50 https://github.com/contao/contao/releases/tag/5.7.12 https://github.com/contao/contao/security/advisories/GHSA-628f-v4f6-p37r	none	no	total
CVE-2026-106509	8,8	Backstage; backstage/plugin-techdocs-node	Improper Control of Generation of Code ('Code Injection'); Improper Neutralization of Special Elements Used in a Template Engine	Prior to 1.14.6	https://github.com/backstage/backstage/commit/02cd7cddb18b687446277b5602adaee7f1d53cbb https://github.com/backstage/backstage/commit/a900a9953c8f7ad3ba1906d1d257725a9996cc9d https://github.com/backstage/backstage/releases/tag/v1.50.5 https://github.com/backstage/backstage/releases/tag/v1.54.6 https://github.com/backstage/backstage/security/advisories/GHSA-8w7q-29mw-qf5c	none	no	partial
CVE-2026-107818	8,4	MariaDB server	External Control of System or Configuration Setting	>= 10.6.1, < 10.6.28; >= 10.11.1, < 10.11.19; >= 11.4.1, < 11.4.13; >= 11.8.1, < 11.8.9; >= 12.3.1, < 12.3.3; >= 13.0.1, < 13.0.2	https://github.com/MariaDB/server/commit/e3d62d4e78fd4941cef3f5053e6a50d0b32d740e https://github.com/MariaDB/server/releases/tag/mariadb-10.11.19 https://github.com/MariaDB/server/releases/tag/mariadb-10.6.28 https://github.com/MariaDB/server/releases/tag/mariadb-11.4.13 https://github.com/MariaDB/server/releases/tag/mariadb-11.8.9 https://github.com/MariaDB/server/releases/tag/mariadb-12.3.3			
CVE-2026-107837	8,2	RIOT	Out-of-bounds Read	2026.07 and earlier	https://github.com/RIOT-OS/RIOT/commit/0cae205cd1d110e0b8f9ce094714598322d56ce2d https://github.com/RIOT-OS/RIOT/pull/22504 https://github.com/RIOT-OS/RIOT/security/advisories/GHSA-m8mc-q4p7-p8j3			
CVE-2026-46570	8,1	In NTFS-3G	Heap-based Buffer Overflow	before 2026.7.7	https://github.com/tuxera/ntfs-3g/releases#release-2026.7.7 https://github.com/tuxera/ntfs-3g/security/advisories/GHSA-m6aq-pv5j-2wxc	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-2026-107826	7,5	OWASP Coraza WAF	Uncontrolled Recursion	>= 3.0.0, < 3.8.1	https://github.com/corazawaf/coraza/commit/814e1898e083d2ff2ceb644382d0da17e930f93f https://github.com/corazawaf/coraza/releases/tag/v3.8.1 https://github.com/corazawaf/coraza/security/advisories/GHSA-6gcq-wc29-5xf2	poc	yes	partial
CVE-2026-107839	7,5	ageLANServer; several Age of Empires and Age of Mythology games	Uncontrolled Resource Consumption	Prior to version 1.15.2	https://github.com/luskaner/ageLANServer/commit/1dd40166a59356865c0a4b1800f32d05dc8bec79 https://github.com/luskaner/ageLANServer/releases/tag/v1.15.2 https://github.com/luskaner/ageLANServer/security/advisories/GHSA-4jfq-pmq9-257h			
CVE-2026-107840	7,5	yopass	Uncontrolled Resource Consumption	Prior to version 14.7.0	https://github.com/jhaals/yopass/commit/61e31ead04a4fc27ce80bed226af41c7c0426ccf https://github.com/jhaals/yopass/commit/78d0c14f7085048130199662a2ec8a18ec8d6ebb https://github.com/jhaals/yopass/pull/3773 https://github.com/jhaals/yopass/releases/tag/14.7.0 https://github.com/jhaals/yopass/security/advisories/GHSA-6r69-c6wg-7q8m	none	yes	partial
CVE-2026-75350	7,5	EIPStackGroup OpENer			https://github.com/EIPStackGroup/OpENer https://github.com/EIPStackGroup/OpENer/blob/master/source/src/cip/cipcommon.c https://github.com/EIPStackGroup/OpENer/blob/master/source/src/enet_encap/cpl.c https://github.com/EIPStackGroup/OpENer/blob/master/source/src/enet_encap/endianness.c https://github.com/EIPStackGroup/OpENer/issues/576			
CVE-2026-75351	7,5	OpENer	Out-of-bounds Read		https://github.com/EIPStackGroup/OpENer https://github.com/EIPStackGroup/OpENer/issues/574	poc	yes	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
Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway CISA	• CVE-2026-107406 • CVE-2026-88771 • CVE-2026-88772 • CVE-2026-88773 • CVE-2026-88774 • CVE-2026-88775 • CVE-2026-88776 • CVE-2026-88777 • CVE-2026-88778 • CVE-2026-88779	https://cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway

Chinese Government-linked Cyber Threat Actors Combine Automated and Hands-on Hacking Tools to Steal Sensitive Data CISA	▪ CVE-2014-6278 ▪ CVE-2015-3306 ▪ CVE-2015-5477 ▪ CVE-2016-3081 ▪ CVE-2019-11510 ▪ CVE-2021-22205 ▪ CVE-2021-3199 ▪ CVE-2023-22894	https://cisa.gov/news-events/cybersecurity-advisories/aa26-281a
---	---	---

News

Η ενότητα "News" συνοψίζει τα πιο σημαντικά γεγονότα της εβδομάδας στον τομέα της κυβερνοασφάλειας. Εδώ θα βρείτε επιθέσεις που ξεχώρισαν, νέες τεχνικές που εντοπίστηκαν, ή ενέργειες από γνωστές ομάδες hacking. Δίνει την απαραίτητη εικόνα του τι συμβαίνει διεθνώς και πού πρέπει να στραφεί η προσοχή.

Σύντομη περιγραφή / Τίτλος	URL
Hackers abuse Google Ads, Bing redirects to push Claude ClickFix attacks	https://bleepingcomputer.com/news/security/hackers-abuse-google-ads-bing-redirects-to-push-claude-clickfix-attacks
FBI Arrests Another ShinyHunters Suspect Reportedly Involved in Its Jobs Portal Hack	https://thehackernews.com/2026/10/fbi-arrests-another-shinyhunters.html
FBI arrests another suspected ShinyHunters hacker after agency breach	https://bleepingcomputer.com/news/security/fbi-arrests-another-suspected-shinyhunters-hacker-after-agency-breach
New GhostAction Attack Compromises Hundreds of GitHub Repos to Steal Secrets	https://cybersecuritynews.com/ghostaction-github-repo-attack
New Agentic AI Red Team Checklist Adds 222 Tests Across 20 Attack Categories	https://cybersecuritynews.com/agentic-ai-red-team-checklist
Wikimedia Says Rogue AI Agents Abused its Platforms	https://infosecurity-magazine.com/news/wikimedia-confirms-platforms-rogue
TP-Link Sued by Four More U.S. States Over Router Security and China Ties	https://thehackernews.com/2026/10/tp-link-sued-by-four-more-us-states.html
Social Engineering AI Agents: The New BEC for 2026	https://darkreading.com/cybersecurity-operations/social-engineering-ai-agents-bec-2026
Google Domains Impacted by Recent ccTLD Hijacks	https://securityweek.com/google-domains-impacted-by-recent-cctld-domain-hijacks
Man admits to running network of 15,000 money mules for cybercriminals	https://bleepingcomputer.com/news/security/ukrainian-russian-dual-citizen-admits-to-laundering-millions-for-cybercriminals
Microsoft: Outdated Windows devices will stop receiving security updates	https://bleepingcomputer.com/news/microsoft/microsoft-outdated-windows-devices-will-lose-security-protection-next-year
UK Allies Warn of Cyber Threat from China's Integrity Technology Group	https://infosecurity-magazine.com/news/uk-allies-threat-china-integrity
AI Training Critical as Governance Challenges Grow	https://infosecurity-magazine.com/news/ai-training-critical-as-governance
US Disrupts Chinese State-Sponsored Hacking Tools	https://securityweek.com/us-disrupts-chinese-state-sponsored-hacking-tools

Three Teams Demonstrate Remote Hacks of Fully Patched Google Pixel 10 at Pwn2Own	https://thehackernews.com/2026/10/three-teams-demonstrate-remote-hacks-of.html
Anthropic Fast-Tracks AI Bug Reports to OSS Maintainers, Taps 11 Firms for OT Security	https://securityweek.com/anthropic-fast-tracks-ai-bug-reports-to-oss-maintainers-taps-11-firms-for-ot-security
Major AI Firms Pledge Data Protection Changes Following ICO Push	https://infosecurity-magazine.com/news/ai-firms-pledge-data-protection
Google Pixel 10 Exploits Earned Hackers \$560,000 at Pwn2Own	https://securityweek.com/google-pixel-10-exploits-earned-hackers-560000-at-pwn2own
FBI disrupts Chinese hacking tools used to breach critical infrastructure	https://bleepingcomputer.com/news/security/fbi-disrupts-chinese-hacking-tools-used-to-breach-critical-infrastructure
'AgentCorruption' Puts AWS Environments at Risk With One Prompt	https://darkreading.com/cloud-security/agentcorruption-aws-environments-at-risk-single-prompt

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
ASOS Breach Reveals the Risks in Customer-Facing SaaS	https://darkreading.com/cyberattacks-data-breaches/asos-breach-risks-customer-facing-saas
ASOS Confirms Data Breach Linked to Stolen Employee Credentials	https://infosecurity-magazine.com/news/asos-data-breach-stolen-employee
EY Data Breach Exposes Goldman Sachs and Man Group Clients' Data	https://cybersecuritynews.com/ey-data-breach-exposed

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
AnyDesk Linux Flaw Lets Remote Attackers Execute Code as Root Without Authentication	https://cybersecuritynews.com/anydesk-linux-vulnerability
Researchers Publish Working Exploit for Pre-Auth AnyDesk Linux Flaw That Gives Root Access	https://thehackernews.com/2026/10/researchers-publish-working-exploit-for.html
Attackers Exploit AhsayCBS Flaws to Deploy XMRig Miners Disguised as Microsoft Edge	https://thehackernews.com/2026/10/attackers-exploit-ahsaycbs-flaws-to.html
Anthropic Launches Free AI Vulnerability Scanner for Open-Source Projects	https://thehackernews.com/2026/10/anthropic-launches-free-ai.html
Max severity SonicWall SMA1000 flaw now exploited in attacks	https://bleepingcomputer.com/news/security/max-severity-sonicwall-sma1000-flaw-now-exploited-in-attacks
Flax Typhoon Exploits Five Flaws as CISA Sets October 11 Deadline for Federal Agencies	https://thehackernews.com/2026/10/flax-typhoon-exploits-five-flaws-as.html

PoC Released for Telegram Desktop Flaw Enabling One-Click File Account Takeover	https://cybersecuritynews.com/poc-released-for-telegram-desktop-flaw
GoBalance Flaw Lets Attackers Hijack .onion Addresses by Recovering Tor-Format Keys	https://thehackernews.com/2026/10/gobalance-flaw-lets-attackers-hijack.html
New Anthropic OSS Scanner Tool to Scan Open-source Repositories for Vulnerabilities	https://cybersecuritynews.com/anthropic-oss-scanner
Citrix warns admins to patch new NetScaler RCE flaw immediately	https://bleepingcomputer.com/news/security/citrix-warns-admins-to-patch-new-netscaler-rce-flaw-immediately
Citrix Urges Immediate Patching of Critical NetScaler Vulnerability	https://securityweek.com/citrix-urges-immediate-patching-of-critical-netscaler-vulnerability
Hackers get \$1,262,000 for 98 zero-days at Pwn2Own Ireland	https://bleepingcomputer.com/news/security/hackers-earn-1262000-for-98-zero-days-at-pwn2own-ireland
Japan Sees Sharp Rise in Web Data Leaks Amid Mobile API Abuse and Metabase Attacks	https://thehackernews.com/2026/10/japan-sees-sharp-rise-in-web-data-leaks.html
Cisco warns of critical flaws allowing Nexus switch takeover	https://bleepingcomputer.com/news/security/cisco-warns-of-critical-flaws-allowing-nexus-switch-takeover
Attackers Target Critical Atlassian Vulnerability Within Hours of PoC Publication	https://securityweek.com/attackers-target-critical-atlassian-vulnerability-within-hours-of-poc-publication
SonicWall and Splunk Patch Critical Vulnerabilities	https://securityweek.com/sonicwall-and-splunk-patch-critical-vulnerabilities
TP-Link Faces State Lawsuits and New Scrutiny Over ISP Router Flaws	https://securityweek.com/tp-link-faces-state-lawsuits-and-new-scrutiny-over-isp-router-flaws
Critical Flaw in Multiple Atlassian Products Exploited in the Wild	https://infosecurity-magazine.com/news/critical-vulnerability-atlassian
Hackers exploit critical Atlassian flaw after public PoC release	https://bleepingcomputer.com/news/security/hackers-exploit-critical-atlassian-flaw-after-public-poc-release
Atlassian Data Center Flaw Draws Exploitation Attempts Within Two Hours of Public Details	https://thehackernews.com/2026/10/atlassian-data-center-flaw-draws.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
Unpatched AhsayCBS flaws exploited to deploy webshells, mine crypto	https://bleepingcomputer.com/news/security/unpatched-ahsaycbs-flaws-exploited-to-deploy-webshells-mine-crypto
Unpatched AhsayCBS Vulnerabilities Exploited in the Wild	https://securityweek.com/unpatched-ahsaycbs-vulnerabilities-exploited-in-the-wild
Citrix Patches Critical NetScaler Flaw That Could Enable RCE in SAML Deployments	https://thehackernews.com/2026/10/citrix-patches-critical-netscaler-flaw.html
Cisco Patches a Dozen Critical Vulnerabilities	https://securityweek.com/cisco-patches-a-dozen-critical-vulnerabilities
SonicWall Patches CVSS 10.0 Pre-Authentication SSRF Flaw in SMA1000 Appliances	https://thehackernews.com/2026/10/sonicwall-patches-cvss-100-pre.html
Unpatched Critical LMCACHE Flaw Lets Unauthenticated Attackers Run Code Remotely	https://thehackernews.com/2026/10/unpatched-critical-lmcache-flaw-lets.html
Chrome 155 Update Patches 247 Vulnerabilities	https://securityweek.com/chrome-155-update-patches-247-vulnerabilities

Atlassian Patches Critical Vulnerability Affecting 8 Products	https://securityweek.com/atlassian-patches-critical-vulnerability-affecting-8-products
---	---

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
Germany arrests alleged core Qilin ransomware member after extradition	https://bleepingcomputer.com/news/security/germany-arrests-alleged-core-qilin-ransomware-member-after-extradition
CastleStealer Malware Uses Browser Protection Bypass and Remote Shell to Expand Attacker Access	https://cybersecuritynews.com/castlestealer-malware
In Other News: AI Used in Korean Bank Breaches, Poem-Guided Botnet, Empire Admin Gets 40 Years	https://securityweek.com/in-other-news-ai-used-in-korean-bank-breaches-poem-guided-botnet-empire-admin-gets-40-years
Q3 2026 Sets New Record for Ransomware Attacks	https://infosecurity-magazine.com/news/q3-new-record-ransomware
Pre-Baked Firmware Malware Hits Budget Android Devices in 150+ Countries	https://securityweek.com/pre-baked-firmware-malware-hits-budget-android-devices-in-150-countries
ThreatsDay: Ransomware Affiliate Betrayal, WhatsApp RAT, Exposed Hacker Tools and 12 More Stories	https://thehackernews.com/2026/10/threatsday-ransomware-affiliate.html
Russia-Aligned UAC-0099 Evolves MATCHBOIL Malware	https://infosecurity-magazine.com/news/russia-aligned-uac-0099-evolves
Alert Overload, Tool Sprawl and Evasive Phishing: The 5 Bottlenecks Slowing Down US SOCs	https://cybersecuritynews.com/alert-overload-tool-sprawl-and-evasive-phishing-the-5-bottlenecks-slowng-down-us-socs
PoeLLM Malware Infects 3,400+ Servers to Expand Crypto Mining Botnet	https://thehackernews.com/2026/10/poellm-malware-infects-3400-servers-to.html
Attackers Hide AI Prompt Injections Inside Phishing Emails	https://infosecurity-magazine.com/news/attackers-hide-ai-prompt

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
Δεν εντοπίστηκαν άρθρα για το καθορισμένο χρονικό διάστημα.	

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 07/10/2026–09/10/2026, 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/