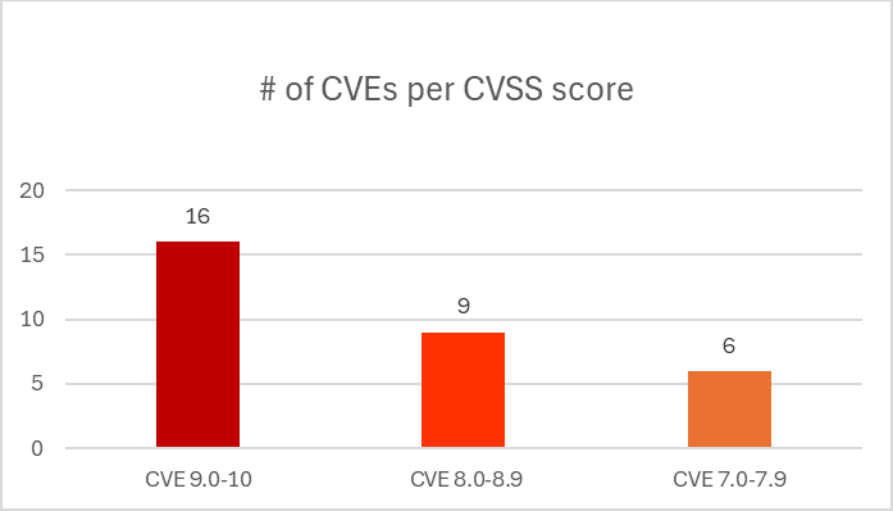
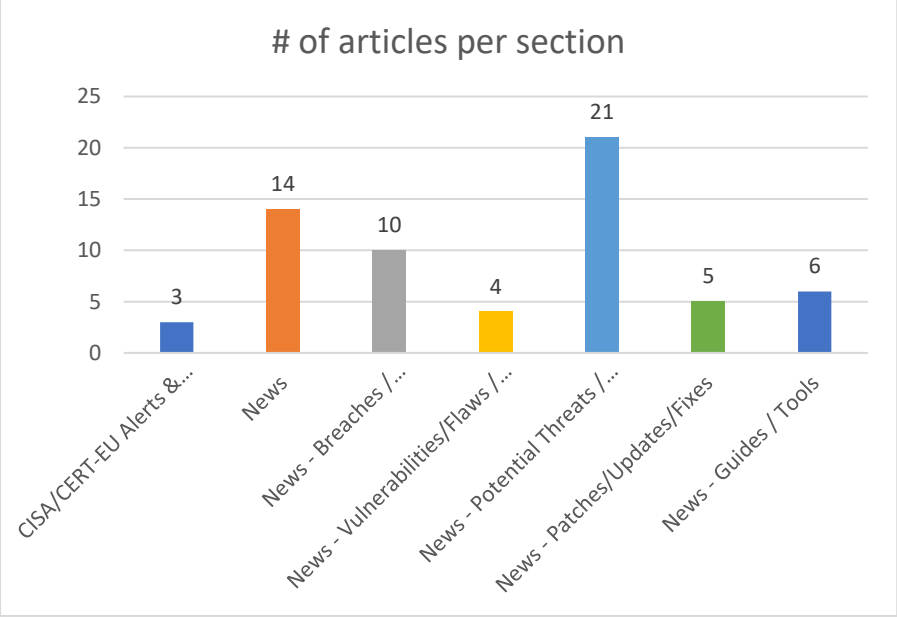
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 28/10/2026 - 30/10/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 8
News 9
Breaches / Compromised / Hacked 10
Vulnerabilities / Flaws / Zero-day 11
Patches / Updates / Fixes 11
Potential threats / Threat intelligence 12
Guides / Tools 13
References 14
Annex – Websites with vendor specific vulnerabilities 15

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)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/cve-2026-61567	10,0	AVideo	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 8.1.0	https://github.com/WWBN/AVideo-Encoder/commit/99b8ad9b66fe5726cababbe29dce9d9695131caa https://github.com/WWBN/AVideo-Encoder/releases/tag/v8.1.0 https://github.com/WWBN/AVideo-Encoder/security/advisories/GHSA-rf63-6vwm-wv8p
https://nvd.nist.gov/vuln/detail/cve-2026-61991	10,0	AjaxLoadMore Cache	Improper Control of Generation of Code ('Code Injection')	AjaxLoadMore Cache <= 3.1.1 versions	https://patchstack.com/database/wordpress/plugin/ajax-load-more-cache/vulnerability/wordpress-ajaxloadmore-cache-plugin-3-1-1-remote-code-execution-rce-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-109516	9,8	Bot for Telegram on WooCommerce plugin for WordPress	Improper Authentication	Bot for Telegram on WooCommerce plugin for WordPress	https://plugins.trac.wordpress.org/browser/bot-for-telegram-on-woocommerce/tags/1.3.0/includes/BFTOW_Telegram.php#L91 https://plugins.trac.wordpress.org/browser/bot-for-telegram-on-woocommerce/tags/1.3.0/includes/BFTOW_Telegram.php#L98 https://plugins.trac.wordpress.org/browser/bot-for-telegram-on-woocommerce/tags/1.3.0/includes/BFTOW_User.php#L149 https://plugins.trac.wordpress.org/browser/bot-for-telegram-on-woocommerce/tags/1.3.0/includes/BFTOW_User.php#L44 https://plugins.trac.wordpress.org/browser/bot-for-telegram-on-woocommerce/tags/1.3.0/includes/BFTOW_User.php#L62 https://plugins.trac.wordpress.org/browser/bot-for-telegram-on-woocommerce/tags/1.3.0/includes/BFTOW_WooCommerce.php#L42 https://www.wordfence.com/threat-intel/vulnerabilities/id/1f6b73e0-c154-4bc4-90bc-0929053b77b0?source=cve

https://nvd.nist.gov/vuln/detail/cve-2026-115245	9,8	Chat AI with Dispatcher WordPress plugin	Unrestricted Upload of File with Dangerous Type	Chat AI with Dispatcher WordPress plugin before 2.4	https://wpscan.com/vulnerability/0981b4a5-dc97-4129-833c-8b297d5200bd/
https://nvd.nist.gov/vuln/detail/cve-2026-61992	9,8	WordPress	Deserialization of Untrusted Data	WordPress <= 4.5.5.3 versions	https://patchstack.com/database/wordpress/plugin/geo-my-wp/vulnerability/wordpress-geo-my-wordpress-plugin-4-5-5-4-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-62004	9,8	Motorix	Deserialization of Untrusted Data	Motorix <= 1.11 versions	https://patchstack.com/database/wordpress/theme/motorix/vulnerability/wordpress-motorix-theme-1-11-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-62015	9,8	Gamezone	Deserialization of Untrusted Data	Gamezone <= 1.1.11 versions	https://patchstack.com/database/wordpress/theme/gamezone/vulnerability/wordpress-gamezone-theme-1-1-11-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-62131	9,8	Zoho Flow	Deserialization of Untrusted Data	Zoho Flow <= 2.14.5 versions	https://patchstack.com/database/wordpress/plugin/zoho-flow/vulnerability/wordpress-zoho-flow-plugin-2-14-5-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-86400	9,8	Dell PowerProtect Data Domain	Improper Authentication	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20	https://www.dell.com/support/kbdoc/en-us/000515178/dsa-2026-416-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-93680	9,8	IBM Langflow OSS	Improper Authentication	IBM Langflow OSS 1.0.0 through 1.12.8	https://www.ibm.com/support/pages/node/7294467
https://nvd.nist.gov/vuln/detail/cve-2026-103799	9,6	Dell PowerProtect Data Domain Management Center	Missing Authorization	Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20	https://www.dell.com/support/kbdoc/en-us/000515178/dsa-2026-416-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-97854	9,3	Yamaha wireless LAN router	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Yamaha wireless LAN router NWR100 provided by Yamaha Corporation	https://jvn.jp/en/vu/JVNVU91027179/ https://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91027179.html
https://nvd.nist.gov/vuln/detail/cve-2026-119128	9,1	ZITADEL	Reliance on Cookies without Validation and Integrity Checking	ZITADEL 4.0.0 before 4.19.5	https://github.com/zitadel/zitadel/security/advisories/GHSA-84fg-x5h4-w8xv https://www.vulncheck.com/advisories/zitadel-4.0.0-before-4.19.5-login-v2-account-takeover-via-forgeable-verificationcheck-cookie
https://nvd.nist.gov/vuln/detail/cve-2026-90717	9,1	Dell PowerProtect Data Domain Management Center	Authentication Bypass by Spoofing	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20	https://www.dell.com/support/kbdoc/en-us/000515178/dsa-2026-416-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities

https://nvd.nist.gov/vuln/detail/cve-2026-90717	9,1	Dell PowerProtect Data Domain Management Center	Authentication Bypass by Spoofing	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20	https://www.dell.com/support/kbdoc/en-us/000515178/dsa-2026-416-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-61707	9,0	SOCFortress CoPilot	Improper Neutralization of Special Elements Used in a Template Engine	Prior to 0.1.76	https://github.com/socfortress/CoPilot/commit/a5ed4a250094d1b6d15ba0ec088dbd773ab1b4e0 https://github.com/socfortress/CoPilot/pull/936 https://github.com/socfortress/CoPilot/security/advisories/GHSA-7q83-228r-wfh5 https://github.com/socfortress/CoPilot/tree/v0.1.76
https://nvd.nist.gov/vuln/detail/cve-2026-118579	8,9	D-Link DIR-505	Hidden Functionality	D-Link DIR-505 1.10B02	https://github.com/Walnut1337/DIR-505_backdoor/tree/main/poc https://vuldb.com/cve/CVE-2026-118579 https://vuldb.com/submit/1025351 https://vuldb.com/vuln/428018 https://vuldb.com/vuln/428018/cti https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/cve-2026-118619	8,8	Ultralytics Google Drive	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Ultralytics Google Drive Download Path Traversal Remote Code Execution Vulnerability	https://www.zerodayinitiative.com/advisories/ZDI-26-818/
https://nvd.nist.gov/vuln/detail/cve-2026-88077	8,8	Microsoft Edge (Chromium-based)	Integer Overflow or Wraparound	Microsoft Edge (Chromium-based)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-88077
https://nvd.nist.gov/vuln/detail/cve-2026-96192	8,8	Microsoft Edge for iOS	Use After Free	Microsoft Edge for iOS	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96192
https://nvd.nist.gov/vuln/detail/cve-2026-96203	8,8	Microsoft Edge (Chromium-based)	Use After Free	Microsoft Edge (Chromium-based)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96203
https://nvd.nist.gov/vuln/detail/cve-2026-118694	8,7	python-markdown2	Inefficient Algorithmic Complexity	python-markdown2 through 2.5.5	https://github.com/trentm/python-markdown2 https://github.com/trentm/python-markdown2/blob/2.5.5/lib/markdown2.py#L1478-L1492 https://github.com/trentm/python-markdown2/blob/2.5.5/lib/markdown2.py#L3029 https://github.com/trentm/python-markdown2/issues/750 https://github.com/trentm/python-markdown2/pull/751 https://www.vulncheck.com/advisories/python-markdown2-through-2.5.5-denial-of-service-via-unclosed-inline-link-destinations

https://nvd.nist.gov/vuln/detail/cve-2026-119052	8,7	llama.cpp	Uncaught Exception	llama.cpp b2877 before b11935	https://github.com/ggml-org/llama.cpp https://github.com/ggml-org/llama.cpp/blob/8542e94350f0ade01644db6f1d1520da3814dafd/ggml/src/ggml-rpc/ggml-rpc.cpp#L344-L356 https://github.com/ggml-org/llama.cpp/commit/7ecb57f7adbea2928aa468ad2aecf05b10725ad4 https://github.com/ggml-org/llama.cpp/pull/31204 https://github.com/ggml-org/llama.cpp/releases/tag/b11935 https://www.vulncheck.com/advisories/llama-cpp-b2877-before-b11935-ggml-rpc-server-dos-via-oversized-recv-msg-length
https://nvd.nist.gov/vuln/detail/cve-2026-61542	8,6	Gearboy	Missing Authentication for Critical Function	Gearboy is a Game Boy, Game Boy Color, and Super Game Boy emulator and debugger with an embedded MCP server	https://github.com/drhelius/Gearboy/commit/e2ead98e2fac41e9df5a499e9e421c6a0e73f1bc https://github.com/drhelius/Gearboy/releases/tag/3.8.7 https://github.com/drhelius/Gearboy/security/advisories/GHSA-fmvx-487g-mrww
https://nvd.nist.gov/vuln/detail/cve-2026-76418	8,6	Cisco	Unchecked Return Value to NULL Pointer Dereference	Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75 https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-76418
https://nvd.nist.gov/vuln/detail/cve-2026-119194	7,5	pyasn1	Inefficient Algorithmic Complexity	pyasn1 is a generic ASN.1 library for Python. From 0.3.3 until 0.6.5	https://github.com/pyasn1/pyasn1/commit/a36e3a3d067148d26197a6b7221fd0e2cde9cc86 https://github.com/pyasn1/pyasn1/pull/132 https://github.com/pyasn1/pyasn1/releases/tag/v0.6.5 https://github.com/pyasn1/pyasn1/security/advisories/GHSA-fm9c-5rcf-2q5p
https://nvd.nist.gov/vuln/detail/cve-2026-114488	7,4	Wildfly	Inclusion of Functionality from Untrusted Control Sphere	-	https://access.redhat.com/security/cve/CVE-2026-114488 https://bugzilla.redhat.com/show_bug.cgi?id=2491619
https://nvd.nist.gov/vuln/detail/cve-2026-119286	7,4	GraphQL-core	Uncontrolled Resource Consumption	GraphQL-core is a Python port of the GraphQL.js reference implementation. From 3.3.0a3 until 3.3.1	https://github.com/graphql-python/graphql-core/commit/3c319fd9f4b8f6c9db4189520561bf8dd0e70be9 https://github.com/graphql-python/graphql-core/issues/287 https://github.com/graphql-python/graphql-core/pull/288 https://github.com/graphql-python/graphql-core/releases/tag/v3.3.1 https://github.com/graphql-python/graphql-core/security/advisories/GHSA-mpqx-q82w-9x46

https://nvd.nist.gov/vuln/detail/cve-2026-110541	7,2	Dell PowerProtect Data Domain	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20	https://www.dell.com/support/kbdoc/en-us/000515178/dsa-2026-416-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-86399	7,2	Dell PowerProtect Data Domain	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20	https://www.dell.com/support/kbdoc/en-us/000515178/dsa-2026-416-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-109822	7,1	Yamaha wireless LAN router	Insecure Storage of Sensitive Information	Yamaha wireless LAN router NWR100	https://jvn.jp/en/vu/JVNVU91027179/ https://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91027179.html
https://nvd.nist.gov/vuln/detail/cve-2026-88941	6,2	Kaspersky	Missing Authentication for Critical Function	Kaspersky Security Center	https://support.kaspersky.com/vulnerability/list-of-advisories/12430#291026

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-48356 Adobe Commerce and Magento Unrestricted Upload of File with Dangerous Type Vulnerability ▪ CVE-2026-111497 Google Brotli Unchecked Return Value Vulnerability	https://www.cisa.gov/news-events/alerts/2026/10/27/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-41709 Broadcom VMWare ESX Insufficient Logging Vulnerability ▪ CVE-2026-46300 Linux Kernel Missing Initialization of a Variable Vulnerability	https://www.cisa.gov/news-events/alerts/2026/10/28/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-97229 GitLab Community Edition and Enterprise Edition Integer Overflow or Wraparound vulnerability ▪ CVE-2026-76418 Cisco Secure Firewall ASA Software and Cisco Secure FTD Software Unchecked Return Value to NULL Pointer Dereference Vulnerability	https://www.cisa.gov/news-events/alerts/2026/10/29/cisa-adds-two-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
Accenture Contractor Allegedly Gave Claude AI Agent Access to Secure Pentagon Network	https://cybersecuritynews.com/accenture-contractor-allegedly-gave-claude-access/
State of Ad Fraud 2026: 52% of Schemes Use AI as Cloaking Loses Ground to iOS Exploits and Messenger Phishing	https://cybersecuritynews.com/state-of-ad-fraud-2026-52-of-schemes-use-ai-as-cloaking-loses-ground-to-ios-exploits-and-messenger-phishing/
Hackers Launch 8,200 DDoS Attacks Every Hour, Cloudflare's Latest Report Reveals	https://cybersecuritynews.com/8200-ddos-attacks-every-hour/
GitHub Launches Copilot Fusion for Smarter and Cheaper AI Coding	https://cybersecuritynews.com/github-launches-copilot-fusion/
Microsoft Urges Entra ID Admins to Migrate from SMS and Voice Authentication to Passkeys	https://cybersecuritynews.com/microsoft-urges-admins-to-migrate-passkeys/
Fortinet Brings AI Agent Security to Oracle Cloud to Block Prompt Injection and Data Leaks	https://cybersecuritynews.com/fortinet-brings-ai-agent-security-to-oracle-cloud/
Beyond the Sandbox Verdict: 3 Questions for Faster SOC Decisions	https://cybersecuritynews.com/beyond-the-sandbox-verdict-3-questions-for-faster-soc-decisions/
FBI Seizes Virtualine Bulletproof Hosting Domain Linked to Ransomware and Cybercrime	https://cybersecuritynews.com/fbi-seizes-virtualine-bulletproof-hosting/
FortiBleed 2.0 Reveals Thousands of Fortinet VPN and Active Directory Credentials in Exposed Configurations	https://cybersecuritynews.com/fortibleed-2-0-exposes-vpn-credentials/
Hackers Hijack Government and School Subdomains to Promote Illegal Gambling Websites	https://cybersecuritynews.com/illegal-gambling-websites/
Hackers Target U.S. Election Commission, Forcing Online System Shutdown Days Before Midterms	https://cybersecuritynews.com/hackers-target-u-s-election-commission-forcing-online-system-shutdown/
Japan's GMO Internet Urges Customers to Shut Down PCs After Hackers Threaten Ransomware Attack	https://cybersecuritynews.com/japans-gmo-internet/
Discord to Make Discoverable Public Server Messages Searchable on Google	https://cybersecuritynews.com/discord-discoverable-server-messages/

Σύντομη περιγραφή / Τίτλος	URL
Before Your SOC Investigates: What 16K+ Security Teams Already Know	https://cybersecuritynews.com/before-your-soc-investigates-what-16k-security-teams-already-know/

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 Actively Exploiting WordPress Remote Code Execution Flaw Just Hours After Patch Release	https://cybersecuritynews.com/wordpress-rce-exploited/
Polymarket Hacked – Users Reported Funds Stolen From Their Wallets	https://cybersecuritynews.com/polymarket-hacked/
World's Largest Crypto Exchange Binance Hacked, Over $5.7 Billion Reportedly Stolen	https://cybersecuritynews.com/binance-hacked/
Hackers Claim Wagyu Crypto Platform Breach as Researchers Find Thousands of Monero Transaction Records	https://cybersecuritynews.com/wagyu-crypto-platform-breach/
Hackers Attack FreePBX Servers With Malware to Steal SIP Credentials for Phone Fraud	https://cybersecuritynews.com/hackers-attack-freepbx-servers/
319 Chrome Extensions Found Hijacking Searches, Affecting 13.4 Million Users	https://cybersecuritynews.com/319-chrome-extensions/
Chinese Hackers Exploit VMware ESXi 0-Day to Hide Malicious Activity on Compromised Servers	https://cybersecuritynews.com/vmware-esx-logging-vulnerability-exploited/
Hackers Leak Records of 41,000 DHS Personnel, Exposing Undercover ICE Agents	https://cybersecuritynews.com/dhs-data-leak/
Coinbase Customer Data Exposed Via Analytics Vendor Amplitude Security Incident	https://cybersecuritynews.com/coinbase-customer-data-exposed/
Sony Suffers Massive Data Breach – 2.58 Million So-net and Plala Users' Data Exposed	https://cybersecuritynews.com/sony-data-breach/

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
WatchGuard Discloses 7 Critical Firewall Flaws Allowing Remote Code Execution and Root-Level Attacks	https://cybersecuritynews.com/watchguard-discloses-critical-firewall-flaws/
TeamViewer Vulnerabilities Could Let Hackers Execute Malicious Code Through Remote Desktop Sessions	https://cybersecuritynews.com/teamviewer-desktop-session-vulnerabilities/
Node2Shell Vulnerability Actively Exploited in the Wild, CISA Warns	https://cybersecuritynews.com/node2shell-vulnerability/
Hackers Actively Exploiting New Oracle EBS RCE Vulnerability	https://cybersecuritynews.com/oracle-ebs-rce-exploited/

Patches / Updates / Fixes

Εδώ θα βρείτε τις πιο πρόσφατες διορθώσεις και ενημερώσεις ασφαλείας από προμηθευτές λογισμικού και hardware. Το περιεχόμενο αφορά συγκεκριμένα bugs ή exploits που έχουν ήδη δημοσιοποιηθεί, μαζί με οδηγίες για το πώς να εφαρμοστούν τα patches.

Σύντομη περιγραφή / Τίτλος	URL
Cisco Secure Firewall 0-Day Vulnerability Exploited in the Wild to Crash SSL VPN Devices	https://cybersecuritynews.com/cisco-secure-firewall-0-day-vulnerability-exploited/
WordPress 7.1.4 Fixes 22 Security Flaws, Including an Unauthenticated RCE Vulnerability	https://cybersecuritynews.com/wordpress-7-1-4-fixes-security-flaws/
Google Fixes 52 Chrome Security Flaws, Including Four Critical Vulnerabilities	https://cybersecuritynews.com/google-fixes-52-chrome-security-flaws/
Veeam Patches Critical Backup & Replication Authorization Bypass Vulnerability	https://cybersecuritynews.com/veeam-patches-authorization-bypass-vulnerability/
Microsoft Releases Emergency Windows Updates to Block Compromised eMudhra Certificates	https://cybersecuritynews.com/microsoft-to-block-emudhra-certificates/

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
CISA Warns of Linux Kernel Missing Initialization Vulnerability Exploited in Attacks	https://cybersecuritynews.com/linux-kernel-missing-initialization-vulnerability/
Claude AI Exploits Linux Kernel Flaw to Execute Root Com-mands Without User Interaction	https://cybersecuritynews.com/linux-kernel-flaw-root-commands/
Zero-Click 'SMS of Death' Flaw Lets Hackers Disrupt Android Phones With a Single Text	https://cybersecuritynews.com/zero-click-android-vulnerability/
Hackers Exploit Critical Cisco SD-WAN 0-Day Flaw to Deploy KeyDrift Malware and Steal Encryption Keys	https://cybersecuritynews.com/critical-cisco-sd-wan-0-day-flaw/
Chinese Hackers Use Secret Silent Train Network to Exploit Zero-Days Against U.S. Government and Defense	https://cybersecuritynews.com/chinese-hackers/
Microsoft Edge 0-Click Exploit Chains Five Flaws to Execute Code and Escape Sandbox	https://cybersecuritynews.com/microsoft-edge-zero-click-exploit/
Hackers Use Fake Cloudflare Verification Pages to Target Windows and Mac Users	https://cybersecuritynews.com/fake-cloudflare-verification/
Hackers Infect 17,960 Android Phones With Banking Trojans, Steal 7.6 Million SMS Messages	https://cybersecuritynews.com/hackers-infect-17960-android-phones/
Hackers Chain PHP2Shell and Linux Kernel Exploits to Gain Root Access on 25 Servers	https://cybersecuritynews.com/php2shell-gained-root-access-on-25-servers/
Researcher Uncovers New 0-click Flaw in Telegram Stickers and Chained Them to Run Code on iOS	https://cybersecuritynews.com/0-click-flaw-in-telegram-stickers/
Researchers Chain Cloudflare Security Flaws to Bypass CSP and Execute Malicious JavaScript	https://cybersecuritynews.com/cloudflare-xss-vulnerability/
OWASP Finds ChatGPT Helped Low-Skilled User Take Over Admin Account in Hacking Test	https://cybersecuritynews.com/owasp-finds-chatgpt-assisted-admin-takeover/
Malicious Firefox Extensions Impersonate Phantom, Jupiter, and Bitget to Steal Crypto Wallet Keys	https://cybersecuritynews.com/malicious-firefox-extensions-3/
Hackers Use Fake Court Notices to Deliver XWorm Malware Through Hidden Windows Scripts	https://cybersecuritynews.com/xworm-malware-3/

Σύντομη περιγραφή / Τίτλος	URL
Claude AI Builds One-Click Chrome and 0-Click Linux Exploit Chains, Bypasses Android Lock Screen	https://cybersecuritynews.com/claude-ai-builds-exploit/
Hackers Compromise Camera Management Software to Deploy Malware on Windows Computers	https://cybersecuritynews.com/camera-management-software/
Hackers Use CyberStrikeAI Agents to Automate Network Scanning, Exploitation, and Data Theft	https://cybersecuritynews.com/hackers-use-cyberstrikeai-agents/
Hackers Hijack 42 GitHub Repositories to Plant Malware Traps for Claude, Gemini, and Cursor Users	https://cybersecuritynews.com/hackers-hijack-42-github-repositories/
Critical UEFI Firmware Flaw Could Expose Millions of Servers to Pre-Boot Code Execution	https://cybersecuritynews.com/uefi-firmware-vulnerability/
Critical GoAhead TLS Flaws Could Expose Hundreds of Millions of Devices to Attacks	https://cybersecuritynews.com/goahead-tls-vulnerabilities/
Researchers Exploit OpenAI API Flaw to Extract Hidden GPT-5.6 Reasoning Traces	https://cybersecuritynews.com/researchers-exploit-openai-api-flaw/

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
NIST Officially Released Guidance for Transition to Post-Quantum Cryptography	https://cybersecuritynews.com/nist-post-quantum-cryptography-guidance/
Top 10 Best Threat Intelligence Platforms (TIP) in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-threat-intelligence-platforms/
Top 10 Best SOAR Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-soar-tools/
Top 10 Best SIEM Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-siem-tools-2/
Top 10 Best Ransomware Recovery Solutions in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-ransomware-recovery-solutions/
Top 9 Best Backup & Recovery Solutions in 2026 [Ranked & Scored]	https://cybersecuritynews.com/top-9-best-backup-recovery-solutions-in-2026-ranked-scored/

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 και αφορούν το διάστημα 24/10/2026–27/10/2026.

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/