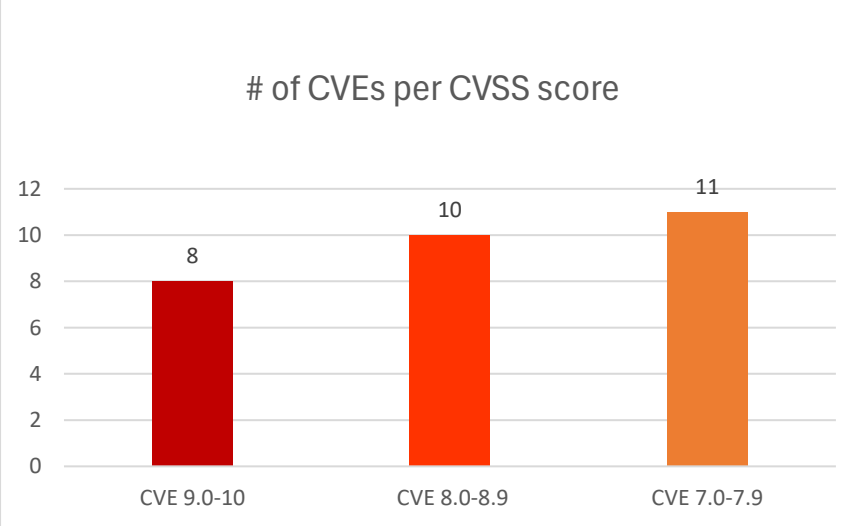
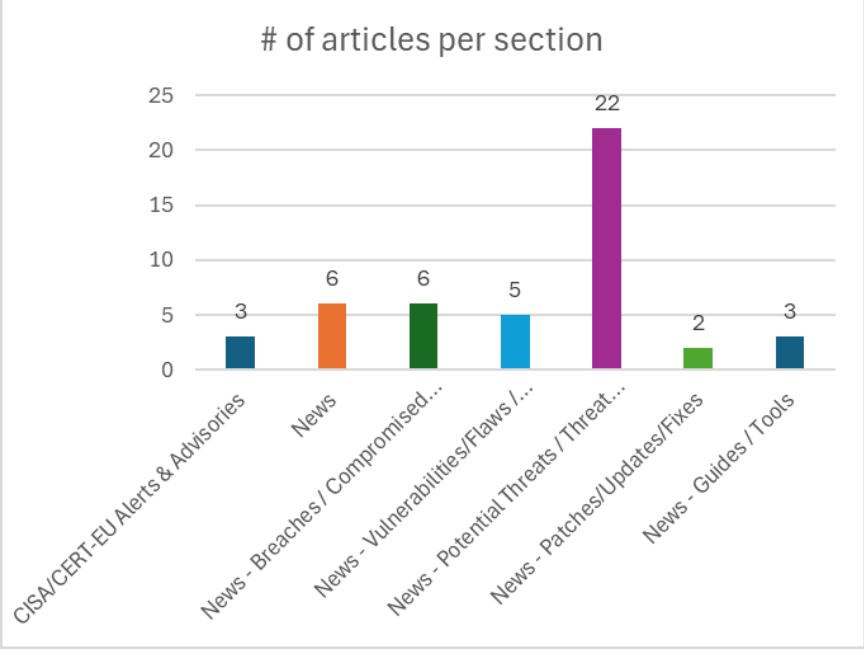
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 08/05/2026 - 12/05/2026





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-2026-42869	10,0	SOCFortress CoPilot	Improper Authentication	Prior to 0.1.57	https://github.com/socfortress/CoPilot/commit/4640511a0cf2e7b144a71375b5b349a8318cb186 https://github.com/socfortress/CoPilot/pull/814 https://github.com/socfortress/CoPilot/security/advisories/GHSA-4gxj-hw3c-3x2x
https://nvd.nist.gov/vuln/detail/CVE-2026-7813	9,9	pgAdmin	Improper Access Control	pgAdmin 4 server mode	https://github.com/pgadmin-org/pgadmin4/pull/9830 P https://github.com/pgadmin-org/pgadmin4/pull/9835
https://nvd.nist.gov/vuln/detail/CVE-2026-0300	9,8	Palo Alto Networks, Inc.	Out-of-bounds Write	A buffer overflow vulnerability in the User-ID™ Authentication Portal (aka Captive Portal) service of Palo Alto Networks PAN-OS software	https://security.paloaltonetworks.com/CVE-2026-0300 https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-0300
https://nvd.nist.gov/vuln/detail/CVE-2026-43465	9,8	Linux kernel	-	-	https://git.kernel.org/stable/c/043bd62f748bc9fd98154037aa598cffbd3c667c https://git.kernel.org/stable/c/7d7342a18fadcdb70a63b3c930dc63528ce51832 https://git.kernel.org/stable/c/db25c42c2e1f9c0d136420fff5e5700f7e771a6f
https://nvd.nist.gov/vuln/detail/CVE-2026-43944	9,6	electerm	Improper Input Validation	From versions 3.0.6 to before 3.8.15	https://github.com/electerm/electerm/commit/8a6a17951e96d715f5a231532bbd8303fe208700 https://github.com/electerm/electerm/commit/a79e06f4a1f0ac6376c3d2411ef4690fa0377742 https://github.com/electerm/electerm/releases/tag/v3.8.15 https://github.com/electerm/electerm/security/advisories/GHSA-mpm8-cx2p-626q
https://nvd.nist.gov/vuln/detail/CVE-2026-45321	9,6	npm registry	Embedded Malicious Code	On 2026-05-11, between approximately 19:20 and 19:26 UTC, 84 malicious versions across 42 @tanstack/* packages were published to the npm registry	https://github.com/TanStack/router/issues/7383 https://github.com/TanStack/router/security/advisories/GHSA-g7cv-rxg3-hmpx
https://www.cve.org/CVERecord?id=CVE-2026-42208	9,3	LiteLLM	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. From version 1.81.16 to before version 1.83.7	github.com: https://github.com/BerriAI/litellm/security/advisories/GHSA-r75f-5x8p-qvmc github.com: https://github.com/BerriAI/litellm/releases/tag/v1.83.7-stable
https://nvd.nist.gov/vuln/detail/CVE-2026-44497	9,1	ZEBRA	Improper Verification of Cryptographic Signature	Prior to zebrad version 4.4.0 and prior to zebra-script version 6.0.0	https://github.com/ZcashFoundation/zebra/security/advisories/GHSA-gq4h-3grw-2rhv
https://nvd.nist.gov/vuln/detail/CVE-2026-8137	8,8	Totolink	Improper Restriction of Operations within the Bounds of a Memory Buffer	Totolink X5000R 9.1.0u.6369_B20230113	https://github.com/Kiciot/cve/issues/4 https://vuldb.com/submit/808863 https://vuldb.com/vuln/361926 https://vuldb.com/vuln/361926/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-8138	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CX12L 16.03.53.12	https://github.com/cve-a/lvdan/issues/6 https://vuldb.com/submit/808867 https://vuldb.com/vuln/361927

					https://vuldb.com/vuln/361927/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-8260	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DCS-935L up to 1.10.01	https://github.com/0xcc12138/DCS-935L-HNAP-Service-CVE https://vuldb.com/submit/809888 https://vuldb.com/vuln/362557 https://vuldb.com/vuln/362557/cti https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-41705	8,6	Spring AI	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	Spring AI's MilvusVectorStore#doDelete(List) implementation is vulnerable to filter-expression injection via unsanitized document IDs. Spring AI 1.0.x: affected from 1.0.0 through latest 1.0.x; upgrade to 1.0.7 or greater. Spring AI 1.1.x: affected from 1.1.0 through latest 1.1.x; upgrade to 1.1.6 or greater.	https://spring.io/security/cve-2026-41705
https://nvd.nist.gov/vuln/detail/CVE-2026-4892	8,4	DHCPv6 implementation of dnsmasq	-	A heap-based out-of-bounds write vulnerability in the DHCPv6 implementation of dnsmasq allows local attackers to execute arbitrary code with root privileges via a crafted DHCPv6 packet.	https://github.com/NixOS/nixpkgs/pull/519082 https://github.com/NixOS/nixpkgs/pull/519093 https://github.com/pi-hole/FTL/releases/tag/v6.6.2 https://lists.thekelleys.org.uk/pipermail/dnsmasq-discuss/2026q2/018471.html https://thekelleys.org.uk/dnsmasq/CVE/ https://www.kb.cert.org/vuls/id/471747
https://nvd.nist.gov/vuln/detail/CVE-2026-43466	8,2	Linux kernel	-	-	https://git.kernel.org/stable/c/1633111d69053512d099658d4a05fc736fab36b0 https://git.kernel.org/stable/c/383b37c04a4827ba60b2bafc1a6cdfd995aed58f https://git.kernel.org/stable/c/6eb68ecc5acc3b319986566c595990b8a7265b23 https://git.kernel.org/stable/c/6f41f7812bfa7f991b732a4b45c5c52fc4be3b4e https://git.kernel.org/stable/c/821f85d619f7f22cda7b9d7de89cf5eeb1d11544 https://git.kernel.org/stable/c/829efcccfa8f69db5dc8332961295587d218cee6 https://git.kernel.org/stable/c/9c5ee9b981ee050b73fdf3f4a2464d6f1a8e10a8 https://git.kernel.org/stable/c/ce1b19dd0684eeb68a124c11085bd611260b36d9
https://nvd.nist.gov/vuln/detail/CVE-2026-44413	8,2	JetBrains TeamCity	Missing Authentication for Critical Function	JetBrains TeamCity before 2026.1 2025.11.5	https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2026-8178	8,1	Amazon Redshift JDBC Driver	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	Amazon Redshift JDBC Driver versions prior to 2.2.2	https://aws.amazon.com/security/security-bulletins/2026-028-aws/ https://github.com/aws/amazon-redshift-jdbc-driver/releases/tag/v2.2.2 https://github.com/aws/amazon-redshift-jdbc-driver/security/advisories/GHSA-wmmv-vvg5-993q
https://nvd.nist.gov/vuln/detail/CVE-2026-32658	8,0	Dell Automation Platform	Missing Authorization	Dell Automation Platform versions prior to 2.0.0.0	https://www.dell.com/support/kbdoc/en-us/000458049/dsa-2026-193-security-update-for-dell-automation-platform-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2026-4802	8,0	Cockpit	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	-	https://access.redhat.com/security/cve/CVE-2026-4802 https://bugzilla.redhat.com/show_bug.cgi?id=2451155 https://github.com/cockpit-project/cockpit/blob/e204cd130/pkg/systemd/logsJournal.jsx#L206-L210
https://nvd.nist.gov/vuln/detail/CVE-2026-43500	7,8	Linux kernel	Out-of-bounds Write	-	https://git.kernel.org/stable/c/3eae0f4f9f7206a4801efa5e0235c25bbd5a412c https://git.kernel.org/stable/c/aa54b1d27fe0c2b78e664a34fd0fdf7cd1960d71

					https://git.kernel.org/stable/c/d45179f8795222ce858770dc619abe51f9d24411 https://github.com/V4bel/dirtyfrag
https://nvd.nist.gov/vuln/detail/CVE-2026-42345	7,7	FastGPT	Server-Side Request Forgery (SSRF)	In versions 4.14.11 and prior	https://github.com/labring/FastGPT/security/advisories/GHSA-jhqw-944x-xh94
https://nvd.nist.gov/vuln/detail/CVE-2026-43469	7,5	Linux kernel	-	-	https://git.kernel.org/stable/c/49f53ee4e25297d886f14e31f355ad1c2735ddfb https://git.kernel.org/stable/c/74c39a47856bddcde7874f2196a00143b5cd0af9 https://git.kernel.org/stable/c/7b6275c80a0c81c5f8943272292dfe67730ce849 https://git.kernel.org/stable/c/7ea69259a60a364f56cf4aa9e2eafb588d1c762b https://git.kernel.org/stable/c/8127b5fec04757c2a41ed65bca0b3266968efd3b https://git.kernel.org/stable/c/8cb6b5d8296b1f99a8d36849901ebabfe3f749db https://git.kernel.org/stable/c/dc3ebd7e2d73dbd4d317785735ffa6c4a6384ddf
https://nvd.nist.gov/vuln/detail/CVE-2026-4890	7,5	DNSSEC	-	A Denial of Service (DoS) vulnerability in the DNSSEC validation of dnsmasq allows remote attackers to cause a denial of service via a crafted DNS packet.	https://github.com/NixOS/nixpkgs/pull/519082 https://github.com/NixOS/nixpkgs/pull/519093 https://github.com/pi-hole/FTL/releases/tag/v6.6.2 https://lists.thekelleys.org.uk/pipermail/dnsmasq-discuss/2026q2/018471.html https://thekelleys.org.uk/dnsmasq/CVE/ https://www.kb.cert.org/vuls/id/471747
https://nvd.nist.gov/vuln/detail/CVE-2026-7287	7,5	Zyxel	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Zyxel NWA1100-N customized firmware version 1.00(AACE.1)C0	https://www.zyxel.com/global/en/support/end-of-life
https://nvd.nist.gov/vuln/detail/CVE-2026-34354	7,4	Akamai Guardicore Platform Agent (GPA) and Zero Trust Client on Linux and macOS	Time-of-check Time-of-use (TOCTOU) Race Condition	This affects Akamai Guardicore Platform Agent 7.0 through 7.3.1 and Akamai Zero Trust Client 6.0 through 6.1.5	https://www.akamai.com/blog/security-research/advisory-cve-2026-34354-guardicore-local-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2026-42264	7,4	Axios	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	From version 1.0.0 to before version 1.15.2	https://github.com/axios/axios/commit/47915144662f2733e6c051bdcb895a8c8f0586aa https://github.com/axios/axios/pull/10779 https://github.com/axios/axios/releases/tag/v1.15.2 https://github.com/axios/axios/security/advisories/GHSA-q8qp-cvcw-x6jj
https://nvd.nist.gov/vuln/detail/CVE-2026-8305	7,3	OpenClaw	Improper Authentication	OpenClaw up to 2026.1.24	https://github.com/Dave-gilmore-aus/security-advisories/blob/main/ClawdBot(aka%20OpenClaw)-Auth-Bypass-SSRF https://github.com/openclaw/openclaw/ https://github.com/openclaw/openclaw/commit/a6653be0265f1f02b9de46c06f52ea7c81a836e6 https://github.com/openclaw/openclaw/issues/13786 https://github.com/openclaw/openclaw/pull/13787 https://github.com/openclaw/openclaw/releases/tag/v2026.2.12 https://vuldb.com/submit/809371 https://vuldb.com/vuln/362590 https://vuldb.com/vuln/362590/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-8265	7,2	Tenda	Improper Neutralization of Special Elements used in	Tenda AC6 15.03.06.23	https://github.com/dxz0069/WAVLINK-WN530H4-Command-Injection-in-set_add_routing/blob/main/Tenda%20AC6V2%20get_log_file%20Command%20Injection%20via%20wans.flag.md

			an OS Command ('OS Command Injection')		https://vuldb.com/submit/810076 https://vuldb.com/vuln/362562 https://vuldb.com/vuln/362562/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-8273	7,2	D-Link	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	D-Link DNS-320 2.06B01	https://github.com/dxz0069/WAVLINK-WN530H4-Command-Injection-in-set_add_routing/blob/main/D-Link%20DNS-320%20%20system_mgraccount_mgrdsk_mgrapp_mgr%20Multiple%20CGI%20OS%20Command%20Injection.md https://vuldb.com/submit/810082 https://vuldb.com/vuln/362570 https://vuldb.com/vuln/362570/cti https://www.dlink.com/
https://www.cve.org/CVERecord?id=CVE-2026-6973	7,2	Ivanti EPMM	Improper input validation	before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1	https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US

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-2026-6973 Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability	https://www.cisa.gov/news-events/alerts/2026/05/07/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-42208 BerriAI LiteLLM SQL Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2026/05/08/cisa-adds-one-known-exploited-vulnerability-catalog
Vulnerability Summary for the Week of May 4, 2026		https://www.cisa.gov/news-events/bulletins/sb26-131

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 Use PlugX-Like DLL Sideloading Chain in Fake Claude Malware Campaign	https://cybersecuritynews.com/hackers-use-plugx-like-dll-sideloading-chain/
Google reCAPTCHA Update Blocks Privacy-Focused Android Users From Sites	https://cybersecuritynews.com/google-recaptcha-update/
Let’s Encrypt Halts Certificate Issuance After Cross-Signed Root Certificate Incident	https://cybersecuritynews.com/lets-encrypt-halts-certificate-issuance/
New ZiChatBot Malware Uses Zulip REST APIs as Command and Control Server	https://cybersecuritynews.com/new-zichatbot-malware-uses-zulip-rest-apis/
Fake Moustache Bypasses Age Verification System Raising Online Safety Act Concerns	https://cybersecuritynews.com/fake-moustache-bypasses-age-verification-system/
New Infostealer Campaign Uses GitHub Releases for Payload Hosting and Evasion	https://cybersecuritynews.com/new-infostealer-campaign-uses-github-releases/

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
ShinyHunters Breaches Instructure Canvas LMS Through Free-For-Teacher Account Program	https://cybersecuritynews.com/shinyhunters-breaches-instructure-canvas-lms/
Crimenetwork Takedown Exposes 22,000 Users and Over 100 Illegal Sellers	https://cybersecuritynews.com/crimenetwork-exposes-22000-users/
JDownloader Downloader Hacked to Infect Users With New Python RAT	https://cybersecuritynews.com/jdownloader-downloader-hacked/
NVIDIA Data Breach Reportedly Exposes Personal Information of GeForce Users	https://cybersecuritynews.com/nvidia-data-breach-geforce-users/
Škoda Security Incident Exposes Customers Data From Online Shop	https://cybersecuritynews.com/skoda-security-incident/
Trellix Breach – RansomHouse Claims Access to Parts of Source Code	https://cybersecuritynews.com/trellix-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
Critical Microsoft 365 Copilot Vulnerabilities Expose sensitive Information	https://cybersecuritynews.com/microsoft-365-copilot-vulnerabilities-data/
Critical Spring Vulnerabilities Expose Arbitrary Files and GCP Secrets	https://cybersecuritynews.com/spring-vulnerabilities-expose-arbitrary-file/
New Ivanti EPMM 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/ivanti-epmm-0-day-exploited/
CISA Warns of Palo Alto PAN-OS Vulnerability Exploited to Gain Root Access	https://cybersecuritynews.com/palo-alto-pan-os-vulnerability-exploited/
New Cisco Network Vulnerability Let Remote Attacker Cause DoS Attack	https://cybersecuritynews.com/cisco-network-vulnerability-dos-attack/

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
Mozilla Patches 423 Firefox Vulnerabilities with Claude Mythos and Other AI Models	https://cybersecuritynews.com/firefox-423-0-day-vulnerabilities/
Multiple Critical Vulnerabilities Patched in Next.js and React Server Components	https://cybersecuritynews.com/next-js-react-server-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
New BitUnlocker Downgrade Attack on Windows 11 Allows Access to Encrypted Disks in 5 Minutes	https://cybersecuritynews.com/bitunlocker-downgrade-attack-on-windows-11/
Hackers Abuse CVE-2026-41940 to Take Over cPanel and WHM Servers	https://cybersecuritynews.com/hackers-abuse-cpanel-and-whm-servers/
84 TanStack npm Packages Hacked in Ongoing Supply-Chain Attack Targeting CI Credentials	https://cybersecuritynews.com/tanstack-npm-packages-hacked/
Popular Go Library fsnotify Raises Supply Chain Alarms After Maintainer Access Changes	https://cybersecuritynews.com/popular-go-library-fsnotify-raises-supply-chain/
Google Warns of Hackers Using AI to Create Working Zero-Day Exploit	https://cybersecuritynews.com/ai-zero-day-exploit/
Hackers Use Fake DeepSeek TUI GitHub Repositories to Deliver Malware	https://cybersecuritynews.com/hackers-use-fake-deepseek-tui-github-repositories/
Trending Hugging Face Repo With 200k Downloads Executes Malware on Windows Machines	https://cybersecuritynews.com/trending-hugging-face-repository-with-200k-downloads/
GhostLock Tool Leverages Windows API to Lock File Access Like Ransomware	https://cybersecuritynews.com/ghostlock-attack/
Hackers Use Weaponized JPEG File to Deploy Trojanized ScreenConnect Malware	https://cybersecuritynews.com/hackers-use-weaponized-jpeg-file/
macOS Malware Leverages Google Ads and Legitimate Claude.ai Shared Chats to Deliver Malware	https://cybersecuritynews.com/macos-malware-leverages-google-ads/
Vidar Malware Targets Browser Credentials, Cookies, Crypto Wallets, and System Data	https://cybersecuritynews.com/vidar-malware-targets-browser-credentials-cookies/
ODINI Malware Uses CPU Magnetic Emissions to Breach Faraday-Shielded Air-Gapped Computers	https://cybersecuritynews.com/odini-malware-air-gapped-computers/
New cPanel and WHM Flaws Enable Code Execution, DoS Attacks	https://cybersecuritynews.com/cpanel-and-whm-flaws/
TCLBANKER Malware Targets Users Through Self-Propagating WhatsApp and Outlook Worm Modules	https://cybersecuritynews.com/tclbanker-malware-targets-users-whatsapp-outlook-worm-modules/
New PamDOORa Backdoor Attacking Linux Systems to Steal SSH Credentials	https://cybersecuritynews.com/new-pamdoora-backdoor-attacking-linux-systems/
Hackers Deploy Modular RAT With Credential Theft and Screenshot Capture Capabilities	https://cybersecuritynews.com/hackers-deploy-modular-rat-with-credential-theft/

Hackers Use Fake OpenClaw Installer to Steal Crypto Wallet and Password Manager Credentials	https://cybersecuritynews.com/hackers-use-fake-openclaw-installer/
Hackers Leveraged Hugging Face and ClawHub With 575+ Malicious Skills to Deploy Malware	https://cybersecuritynews.com/hackers-leverage-hugging-face-and-clawhub/
Hackers Abuse Signed Logitech Installer to Deploy TCLBANKER Banking Trojan	https://cybersecuritynews.com/hackers-abuse-signed-logitech-installer-tclbanker/
New PCPJack Worm Targets Docker, Kubernetes, Redis, and MongoDB for Credential Theft	https://cybersecuritynews.com/new-pcpjack-worm-targets-docker/
New NWHStealer Delivery Chain Uses Bun Loader, Anti-VM Checks, and Encrypted C2	https://cybersecuritynews.com/new-nwhstealer-delivery-chain-uses-bun-loader/
Dirty Frag Linux Vulnerability Let Attackers Gain Root Privileges – PoC Released	https://cybersecuritynews.com/dirty-frag-linux-vulnerability/

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
10 Best Full Disk Encryption Tools in 2026	https://cybersecuritynews.com/best-full-disk-encryption-tools/
Top 10 Best Interactive Malware Analysis Tools in 2026	https://cybersecuritynews.com/best-interactive-malware-analysis-tools/
DarkMoon AI-Powered Autonomous Penetration Testing Platform With 50+ Tools	https://cybersecuritynews.com/darkmoon-penetration-testing-platform/

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/