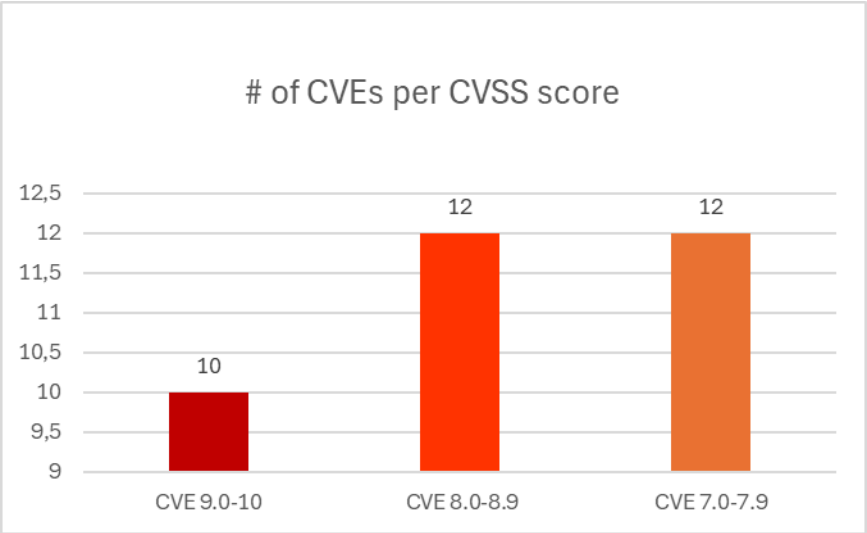
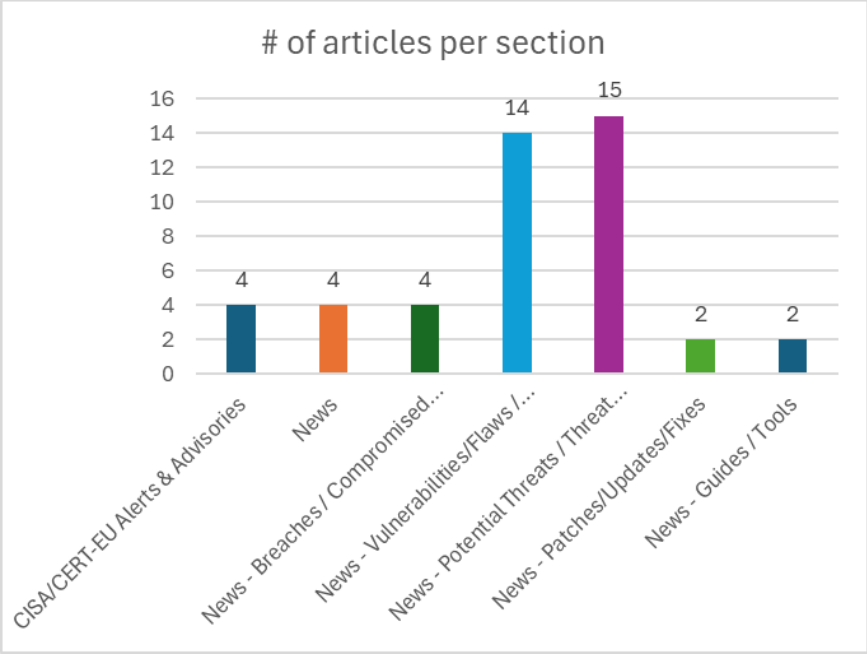
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 29/04/2026 - 01/05/2026





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-2026-30893	9,9	Wazuh	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	From version 4.4.0 to before version 4.14.4	https://github.com/wazuh/wazuh/releases/tag/v4.14.4 https://github.com/wazuh/wazuh/security/advisories/GHSA-m8rw-v4f6-8787
https://nvd.nist.gov/vuln/detail/CVE-2018-25316	9,8	Tenda	Authentication Bypass by Spoofing	Tenda W308R v2 V5.07.48	https://www.exploit-db.com/exploits/44373 https://www.vulncheck.com/advisories/tenda-w308r-v2-cookie-session-weakness-dns-change
https://nvd.nist.gov/vuln/detail/CVE-2018-25317	9,8	Tenda	Authentication Bypass by Spoofing	Tenda W3002R/A302/W309R wireless routers version V5.07.64_en	https://www.exploit-db.com/exploits/44380 https://www.vulncheck.com/advisories/tenda-w3002r-a302-w309r-64-en-cookie-session-weakness-dns-change
https://nvd.nist.gov/vuln/detail/CVE-2018-25318	9,8	Tenda	Authentication Bypass by Spoofing	Tenda FH303/A300 firmware V5.07.68_EN	https://www.exploit-db.com/exploits/44381 https://www.vulncheck.com/advisories/tenda-fh303-a300-68-en-cookie-session-weakness-dns-change
https://nvd.nist.gov/vuln/detail/CVE-2025-71284	9,8	Synway SMG Gateway Management Software	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	-	https://github.com/projectdiscovery/nuclei-templates/blob/main/http/vulnerabilities/synway/synwaysmg-radius-rce.yaml https://mp.weixin.qq.com/s/PyepoFSuQ63E3RnpQa9nsA https://mrxn.net/jswz/synway-9-2radius-rce.html https://www.synway.net/ https://www.vulncheck.com/advisories/synway-smg-gateway-management-software-os-command-injection-via-radius-address
https://nvd.nist.gov/vuln/detail/CVE-2026-36841	9,8	TOTOLINK	Improper Neutralization of Special Elements used in a Command ('Command Injection')	TOTOLINK N200RE V5	https://github.com/0xmania/cve/tree/main/TOTOLINK-N200RE_V5-cstecgi-formMapDelDevice-CommandInjection
https://nvd.nist.gov/vuln/detail/CVE-2026-41940	9,8	cPanel and WHM	Missing Authentication for Critical Function	cPanel and WHM versions after 11.40	https://docs.cpanel.net/release-notes/release-notes https://docs.wpsquared.com/changelogs/versions/changelog/#13617 https://github.com/watchtowrlabs/watchTowr-vs-cPanel-WHM-AuthBypass-to-RCE.py https://support.cpanel.net/hc/en-us/arti-

					cles/40073787579671-cPanel-WHM-Security-Update-04-28-2026 https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-41940 https://www.namecheap.com/status-updates/ongoing-critical-security-vulnerability-in-cpanel-april-28-2026 https://www.vulncheck.com/advisories/cpanel-and-whm-authentication-bypass-via-login-flow
https://nvd.nist.gov/vuln/detail/CVE-2026-7538	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A8000RU 7.1cu.643_b20200521	https://github.com/Litengzheng/vuldb_new2/blob/main/A8000RU/vul_329/README.md https://vuldb.com/submit/804321 https://vuldb.com/vuln/360354 https://vuldb.com/vuln/360354/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-7546	9,8	Totolink	Improper Restriction of Operations within the Bounds of a Memory Buffer	Totolink NR1800X 9.1.0u.6279_B20210910	https://github.com/newym/cve/blob/main/totolinknr1800x.md https://vuldb.com/submit/804404 https://vuldb.com/vuln/360357 https://vuldb.com/vuln/360357/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-42523	9,0	Jenkins	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Jenkins GitHub Plugin 1.46.0 and earlier	https://www.jenkins.io/security/advisory/2026-04-29/#SECURITY-3704
https://nvd.nist.gov/vuln/detail/CVE-2026-6389	8,8	IBM Turbonomic prometurbo agent	Improper Privilege Management	IBM Turbonomic prometurbo agent 8.16.0 through 8.17.6	https://www.ibm.com/support/pages/node/7270720
https://nvd.nist.gov/vuln/detail/CVE-2026-6543	8,8	IBM Langflow Desktop	Improper Control of Generation of Code ('Code Injection')	IBM Langflow Desktop 1.0.0 through 1.8.4	https://www.ibm.com/support/pages/node/7271092
https://nvd.nist.gov/vuln/detail/CVE-2026-7420	8,8	UTT	Improper Restriction of Operations within the Bounds of a Memory Buffer	UTT HiPER 1250GW up to 3.2.7-210907-180535	https://github.com/kirlic123/IOTvuln-er/blob/main/4035/5/5.md https://vuldb.com/submit/803997 https://vuldb.com/vuln/360157 https://vuldb.com/vuln/360157/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-7470	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda 4G300 US_4G300V1.0Mt_V1.01.42_CN_TDC01	https://github.com/Axelioc/CVE/blob/main/Tenda/US_4G300/sub_427C3C/sub_427C3C.md https://vuldb.com/submit/804269 https://vuldb.com/vuln/360206 VulDB https://vuldb.com/vuln/360206/cti https://www.tenda.com.cn/

https://nvd.nist.gov/vuln/detail/CVE-2026-7512	8,8	UTT	Improper Restriction of Operations within the Bounds of a Memory Buffer	UTT HiPER 1200GW up to 2.5.3-1703	https://github.com/kirlic123/IOTvuln-er/tree/main/4035/3 https://vuldb.com/submit/803995 https://vuldb.com/vuln/360323 https://vuldb.com/vuln/360323/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-7513	8,8	UTT	Improper Restriction of Operations within the Bounds of a Memory Buffer	UTT HiPER 1200GW up to 2.5.3-170306	https://github.com/kirlic123/IOTvuln-er/blob/main/4035/4/4.md https://vuldb.com/submit/803996 https://vuldb.com/vuln/360324 https://vuldb.com/vuln/360324/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-7548	8,8	Totolink	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Totolink NR1800X 9.1.0u.6279_B20210910	https://github.com/newym/cve/blob/main/totolink%20nr1800x%20command%20injection.md https://vuldb.com/submit/804417 https://vuldb.com/vuln/360358 https://vuldb.com/vuln/360358/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2018-25301	8,4	Easy MPEG to DVD Burner	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Easy MPEG to DVD Burner 1.7.11	https://downloads.tomsguide.com/MPEG-Easy-Burner,0301-10418.html https://www.exploit-db.com/exploits/44565 https://www.vulncheck.com/advisories/easy-mpeg-to-dvd-burner-seh-local-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2026-28221	8,2	Wazuh	Stack-based Buffer Overflow	From version 4.8.0 to before version 4.14.4	https://github.com/wazuh/wazuh/releases/tag/v4.14.4 https://github.com/wazuh/wazuh/security/advisories/GHSA-q9vv-7w4c-f4cm
https://nvd.nist.gov/vuln/detail/CVE-2026-7424	8,1	FreeRTOS-Plus-TCP	Integer Underflow (Wrap or Wraparound)	FreeRTOS-Plus-TCP before V4.4.1 and V4.2.6	https://aws.amazon.com/security/security-bulletins/2026-022-aws/ https://github.com/FreeRTOS/FreeRTOS-Plus-TCP/releases/tag/V4.2.6 https://github.com/FreeRTOS/FreeRTOS-Plus-TCP/releases/tag/V4.4.1 https://github.com/FreeRTOS/FreeRTOS-Plus-TCP/security/advisories/GHSA-wrhm-c99p-2p8g
https://nvd.nist.gov/vuln/detail/CVE-2026-7426	8,1	FreeRTOS-Plus-TCP	Out-of-bounds Write	FreeRTOS-Plus-TCP before V4.2.6 and V4.4.1	https://aws.amazon.com/security/security-bulletins/2026-023-aws/ https://github.com/FreeRTOS/FreeRTOS-Plus-TCP/releases/tag/V4.2.6 https://github.com/FreeRTOS/FreeRTOS-Plus-TCP/releases/tag/V4.4.1 https://github.com/FreeRTOS/FreeRTOS-Plus-TCP/security/advisories/GHSA-97qg-4359-xm3x
https://nvd.nist.gov/vuln/detail/CVE-2026-42524	8,0	Jenkins HTML Publisher Plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Jenkins HTML Publisher Plugin 427 and earlier	https://www.jenkins.io/security/advisory/2026-04-29/#SECURITY-3706

https://nvd.nist.gov/vuln/detail/CVE-2026-5405	7,8	Wireshark	Heap-based Buffer Overflow	Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14	https://gitlab.com/wireshark/wireshark/-/issues/21105 https://www.wireshark.org/security/wnpa-sec-2026-17.html
https://nvd.nist.gov/vuln/detail/CVE-2025-51846	7,5	CryptPad	Allocation of Resources Without Limits or Throttling	CryptPad 2025.3.1	https://github.com/JohnPerifanis/cryptpad-cve-2025-51846-advisory/blob/main/README.md https://github.com/cryptpad/cryptpad/pull/2239/changes/1e0c06ad8a0c5dab795f85f9730ec2693320c62e https://raw.githubusercontent.com/cisa-gov/CSAF/develop/csaf_files/IT/white/2026/va-26-119-01.json https://www.cve.org/CVERecord?id=CVE-2025-51846
https://nvd.nist.gov/vuln/detail/CVE-2026-36837	7,5	TOTOLINK	Stack-based Buffer Overflow	TOTOLINK A3002RU V3 <= V3.0.0-B20220304.1804	https://github.com/0xmania/cve/tree/main/TOTOLINK-A3002RUV3.0-boa-formMapDelDevice-StackOverflow
https://nvd.nist.gov/vuln/detail/CVE-2026-36957	7,5	Dbit N300 T1 Pro	Uncontrolled Resource Consumption	Dbit N300 T1 Pro Easy Setup Wireless Wi-Fi Router V1.0.0	http://dbit.com https://github.com/kirubel-cve/CVE-2026-36957
https://nvd.nist.gov/vuln/detail/CVE-2026-36958	7,5	U-SPEED	Uncontrolled Resource Consumption	U-SPEED N300 V1.0.0 wireless router	http://u-speed.com https://github.com/kirubel-cve/CVE-2026-36958
https://nvd.nist.gov/vuln/detail/CVE-2026-42403	7,5	Apache Neethi	Uncontrolled Resource Consumption	Users are recommended to upgrade to version 3.2.2, which fixes this issue	https://lists.apache.org/thread/zm6t8skkk-skjwk1881l4m4n0l7dqclzo
https://nvd.nist.gov/vuln/detail/CVE-2026-42520	7,5	Jenkins Credentials Binding Plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Jenkins Credentials Binding Plugin 719.v80e905ef14eb_ and earlier	https://www.jenkins.io/security/advisory/2026-04-29/#SECURITY-3672
https://nvd.nist.gov/vuln/detail/CVE-2026-41882	7,4	JetBrains IntelliJ IDEA	Improper Link Resolution Before File Access ('Link Following')	JetBrains IntelliJ IDEA before 2024.3.7.1, 2025.1.7.1, 2025.2.6.2, 2025.3.4.1, 2026.1.1	https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2026-7461	7,2	FSx Windows File Server	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Improper neutralization of inputs used in an OS command in the FSx Windows File Server volume mounting component in Amazon ECS Agent on Windows before version 1.103.0	https://aws.amazon.com/security/security-bulletins/2026-024-aws/ https://github.com/aws/amazon-ecs-agent/releases/tag/v1.103.0 https://github.com/aws/amazon-ecs-agent/security/advisories/GHSA-fc67-c4hg-q653
https://nvd.nist.gov/vuln/detail/CVE-2025-13030	7,1	django-mdeditor	Missing Authentication for Critical Function	All versions of the package django-mdeditor are vulnerable to Missing Authentication for Critical Function in the image upload endpoint	https://github.com/pylixm/django-mdeditor/blob/e8dd73fb8571ddff2e7a20a4bfa88c376cc33b62/mdeditor/views.py%23L25 https://github.com/pylixm/django-mdeditor/commit/3e80f9ed-cabc5d2fc136b05a501964b8a5e97cfe

					https://github.com/pylixm/django-mdeditor/issues/151 https://github.com/pylixm/django-mdeditor/pull/185 https://security.snyk.io/vuln/SNYK-PYTHON-DJANGOMDEDITOR-8630926
https://nvd.nist.gov/vuln/detail/CVE-2026-35155	**7,1**	Dell iDRAC10	Insufficiently Protected Credentials	Dell iDRAC10, versions 1.20.70.50 and 1.30.05.10	https://www.dell.com/support/kbdoc/en-us/000452298/dsa-2026-187-security-update-for-dell-idrac10-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2026-5656	**7,0**	Wireshark	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Wireshark 4.6.0 to 4.6.4 and 4.4.0 to 4.4.14	https://gitlab.com/wireshark/wireshark/-/issues/21115 https://www.wireshark.org/security/wnpa-sec-2026-21.html

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-2024-1708 ConnectWise ScreenConnect Path Traversal Vulnerability ▪ CVE-2026-32202 Microsoft Windows Protection Mechanism Failure Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/28/cisa-adds-two-known-exploited-vulnerabilities-catalog
Adapting Zero Trust Principles to Operational Technology		https://www.cisa.gov/resources-tools/resources/adapting-zero-trust-principles-operational-technology
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-41940 WebPros cPanel & WHM and WP2 (WordPress Squared) Missing Authentication for Critical Function Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/30/cisa-adds-one-known-exploited-vulnerability-catalog
Careful Adoption of Agentic AI Services		https://www.cisa.gov/resources-tools/resources/careful-adoption-agentic-ai-services

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
Ransomware Victims Jump to 7,831 as AI Crime Tools Scale Global Attacks	https://cybersecuritynews.com/ransomware-victims-jump-to-7831-as-ai-crime-tools/
Anthropic Launches Claude Security in Public Beta for Enterprise Customers	https://cybersecuritynews.com/claude-security-public-beta/
OpenAI Releases 5-Point Action Plan to Strengthen AI-Powered Cyber Defense	https://cybersecuritynews.com/openai-5-point-action-plan/
Europol Busts €50 Million Online Fraud Network Running Corporate-Style Scam Call Centres	https://cybersecuritynews.com/europol-busts-e50-million-online-fraud-network/

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
Popular Python Package lightning Hacked in Supply Chain Attack	https://cybersecuritynews.com/python-package-lightning-hacked/
WordPress Plugin Hacked Since 2020 to Inject Malicious Code Silently	https://cybersecuritynews.com/wordpress-plugin-hacked/
SAP npm Packages Compromised to Harvest Developer and CI/CD Secrets	https://cybersecuritynews.com/sap-npm-packages-compromised/
Vimeo Confirms Data Breach – Hackers Accessed Users Database	https://cybersecuritynews.com/vimeo-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
Critical Wireshark Vulnerabilities Let Attackers Execute Arbitrary Code Via Malformed Packets	https://cybersecuritynews.com/wireshark-vulnerabilities-code-execution/
Microsoft Windows 11 April 2026 Security Update Breaks Third-Party Backup Applications	https://cybersecuritynews.com/windows-11-backup-applications/
Google Gemini CLI Vulnerabilities Allow Attackers to Execute Commands on Host Systems	https://cybersecuritynews.com/google-gemini-cli-vulnerabilities/
Qinglong Task Scheduler RCE Vulnerabilities Exploited in the Wild	https://cybersecuritynews.com/qinglong-task-scheduler-rce-vulnerabilities/
CISA Warns of ConnectWise ScreenConnect Vulnerability Exploited in Attacks	https://cybersecuritynews.com/connectwise-screenconnect-vulnerability/
ProFTPD's SQL Injection Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/proftpds-sql-injection-vulnerability/
SonicWall SonicOS Vulnerabilities Allow Attackers to Bypass Access Controls and Crash Firewall	https://cybersecuritynews.com/sonicwall-sonicos-vulnerabilities/
cPanel 0-Day Authentication Bypass Vulnerability Actively Exploited in the Wild — PoC Released	https://cybersecuritynews.com/cpanel-0-day-authentication-bypass-vulnerability/
Cursor AI Extension Access Developer Tokens Leads to Full Credential Compromise	https://cybersecuritynews.com/cursor-ai-extension-access-developer-tokens/
Linux Kernel 0-Day "Copy Fail" Roots Every Major Distribution Since 2017	https://cybersecuritynews.com/linux-kernel-0-day-copy-fail/
Cursor AI Coding Agent Vulnerability Allow Attackers to Execute Code on Developer's Machine	https://cybersecuritynews.com/cursor-ai-coding-agent-vulnerability/
CISA Warns Microsoft Windows Shell 0-click Vulnerability Exploited in Attacks	https://cybersecuritynews.com/windows-shell-0-click-vulnerability/

Hugging Face LeRobot Vulnerability Enables Unauthenticated RCE Attacks	https://cybersecuritynews.com/hugging-face-lerobot-vulnerability/
Critical Chrome Vulnerabilities Enables Remote Code Execution Attacks	https://cybersecuritynews.com/chrome-vulnerabilities-2/

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
Jenkins Patches High-Severity Plugin Flaws Including Path Traversal and Stored XSS	https://cybersecuritynews.com/jenkins-patches-multiple-vulnerabilities-2/
cPanel Warns of Critical Authentication Flaw – Emergency Patch Released	https://cybersecuritynews.com/cpanel-authentication-flaw/

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
Deep#Door Stealer Harvests Browser Passwords, Cloud Tokens, SSH Keys, and Wi-Fi Credentials	https://cybersecuritynews.com/deepdoor-stealer-harvests-browser-passwords/
China-Aligned Attackers Use ShadowPad, IOX Proxy, and WMIC in Multi-Stage Espionage Campaign	https://cybersecuritynews.com/china-aligned-attackers-use-multi-stage-espionage-campaign/
New Fake CAPTCHA Campaign Uses SMS Pumping Fraud to Run Up Victims' Phone Bills	https://cybersecuritynews.com/new-fake-captcha-campaign-uses-sms-pumping/
Qilin Ransomware Enumerates RDP Authentication History on a Compromised Server	https://cybersecuritynews.com/qilin-ransomware-enumerates-rdp-authentication/
Targeted Large-Scale Campaign Attacking U.S. Organizations with Fake Event Invitations	https://cybersecuritynews.com/campaign-attacking-u-s-organizations-with-fake-event-invitations/
New PhaaS Platform Phoenix Drives Brand-Impersonation Smishing Across Finance, Telecom, and Logistics	https://cybersecuritynews.com/new-phaas-platform-phoenix/
Claude-Generated Commit Adds PromptMink Malware to Crypto Trading Agent	https://cybersecuritynews.com/claude-generated-commit-adds-promptmink-malware/
Novel KarstoRAT RAT Enables Webcam Monitoring, Audio Recording, and Remote Payload Execution	https://cybersecuritynews.com/novel-karstorat-rat-enables-webcam-monitoring/
Malicious npm Package Brand-Squats TanStack Exfiltrate Developer Secrets	https://cybersecuritynews.com/malicious-npm-package-brand-squats-tanstack/
New EtherRAT Variant Uses Trojanized Tftpd64 Installer to Bridge Web2 Malware and Web3 Theft	https://cybersecuritynews.com/new-etherrat-variant-uses-trojanized-tftpd64-installer/

Lazarus Hackers Attacking macOS Users With ‘Mach-O Man’ Malware Kit	https://cybersecuritynews.com/mach-o-man-macos-malware-lazarus/
SLOTAGENT Malware Uses API Hashing and Encrypted Strings to Hinder Reverse Engineering	https://cybersecuritynews.com/slotagent-malware-uses-api-hashing/
Minecraft Players Targeted by LofyStealer Using Node.js Loader and In-Memory Browser Injection	https://cybersecuritynews.com/minecraft-players-targeted-by-lofystealer/
New VECT 2.0 Ransomware Destroys Files Over 128 KB Across Windows, Linux, and ESXi	https://cybersecuritynews.com/new-vect-2-0-ransomware-destroys-files/
New BlueNoroff Campaign Uses Fileless PowerShell and AI-Generated Zoom Lures	https://cybersecuritynews.com/new-bluenoroff-campaign-uses-fileless-powershell/

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
FBI and CISA Released Zero Trust Principles Implementation Guide for OT Environments	https://cybersecuritynews.com/fbi-cisa-released-zero-trust-principles/
CVE MCP Server Turns Claude Into a Fully Capable Security Analyst With 27 Tools Across 21 APIs	https://cybersecuritynews.com/cve-mcp-server-and-claude/

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/