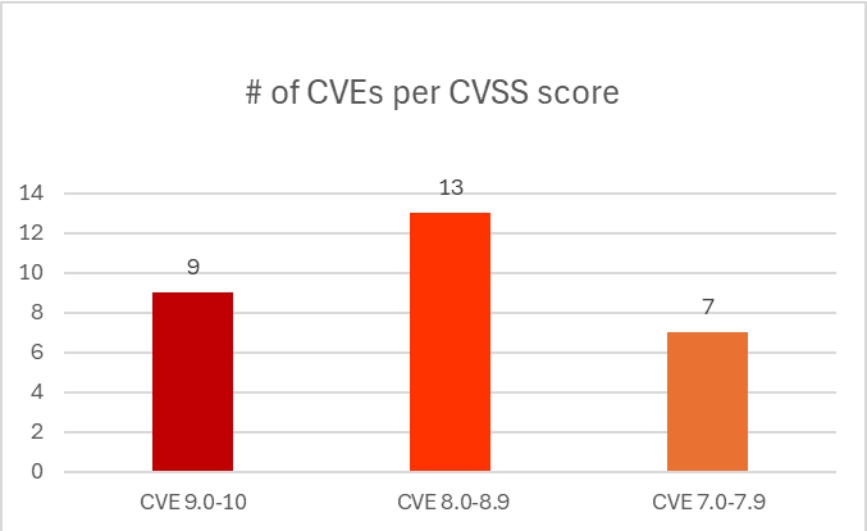
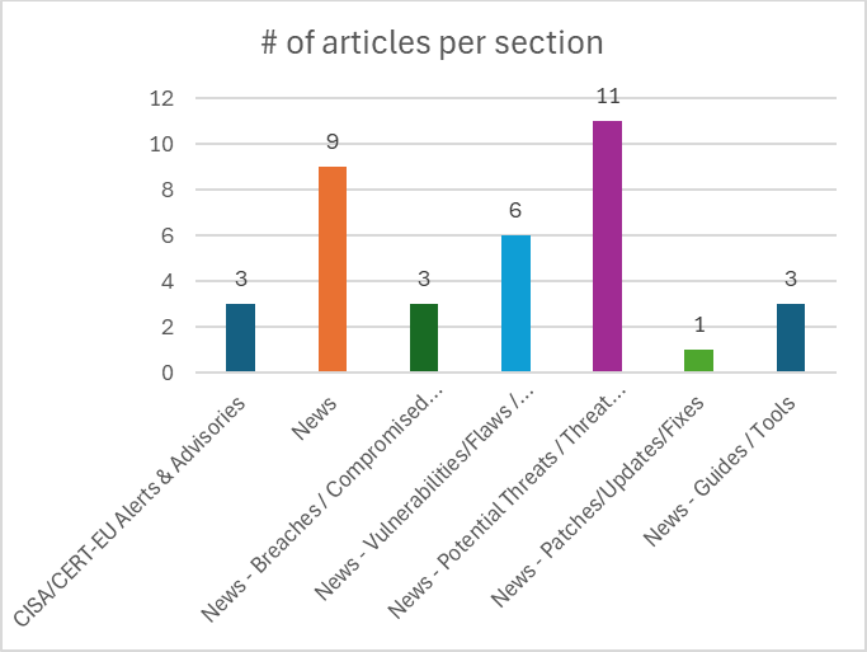
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 11/07/2026 - 14/07/2026





Contents

Common Vulnerabilities and Exposures (CVEs)

Η ενότητα αυτή εστιάζει σε ευπάθειες που έχουν καταχωρηθεί πρόσφατα και αξιολογούνται ως σοβαρές, με βάση τη βαθμολογία CVSS. Παρουσιάζονται με σαφήνεια τα συστήματα ή εφαρμογές που επηρεάζονται, ο τύπος της ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

URL ευπάθειας (NIST NVD)	CVSSv 3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-44747	9,9	SAP NetWeaver Application Server ABAP	Out-of-bounds Write	SAP NetWeaver Application Server ABAP	https://me.sap.com/notes/3747367 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2026-61445	9,9	PraisonAI	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	PraisonAI before 4.6.78	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-9mp3-24cc-77mg https://www.vulncheck.com/advisories/praisonai-before-arbitrary-file-write-and-command-execution
https://nvd.nist.gov/vuln/detail/CVE-2026-15511	9,8	Comfast CF-WR631AX	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Comfast CF-WR631AX V3 up to 2.7.0.8	https://github.com/luminarydawn/cve/tree/main/Command%20Injection%20in%20Comfast%20CF-WR631AX%20V3%20%E2%80%94%20WiFi%20Portal%20Image%20Upload%20(CWE-78) https://vuldb.com/cve/CVE-2026-15511 https://vuldb.com/submit/846719 https://vuldb.com/vuln/377840 https://vuldb.com/vuln/377840/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-60121	9,8	Vitec Flamingo	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Vitec Flamingo 4.12.2	https://damiri.fr/en/cve/CVE-2026-60121 https://www.vitec.com/solutions/iptv-distribution https://www.vulncheck.com/advisories/vitec-flamingo-unauthenticated-os-command-injection-via-ping-php
https://nvd.nist.gov/vuln/detail/CVE-2026-61500	9,8	Rejetto HFS	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	Rejetto HFS 3.0.0 through 3.2.0	https://github.com/rejetto/hfs/releases/tag/v3.2.1 https://www.vulncheck.com/advisories/rejetto-hfs-session-forgery-via-predictable-signing-key
https://nvd.nist.gov/vuln/detail/CVE-2026-14453	9,6	Centreon	Improper Control of Generation of Code ('Code Injection')	Centreon	https://github.com/centreon/centreon/releases
https://nvd.nist.gov/vuln/detail/CVE-2026-56260	9,1	Crawl4AI	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Crawl4AI before 0.8.7	https://github.com/unclecode/crawl4ai https://github.com/unclecode/crawl4ai/security/advisories/GHSA-365w-hqf6-vxfg https://www.vulncheck.com/advisories/crawl4ai-arbitrary-file-write-via-output-path-parameter
https://nvd.nist.gov/vuln/detail/CVE-2026-56372	9,1	ImageMagick	Heap-based Buffer Overflow	ImageMagick before 7.1.2-19	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-8vfj-q2cp-5m5j https://www.vulncheck.com/advisories/imagemagick-heap-buffer-overflow-read-via-unrecognized-magnify-method

https://nvd.nist.gov/vuln/detail/CVE-2026-62327	9,1	9Router	Missing Authentication for Critical Function	9Router through version 0.4.41	https://github.com/decolua/9router/security/advisories/GHSA-vjc7-jrh9-9j86 https://www.vulncheck.com/advisories/9router-unauthenticated-api-key-exposure-via-api-usage-stats
https://nvd.nist.gov/vuln/detail/CVE-2026-15481	8,8	Trendnet	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Trendnet TEW-635BRM up to 1.00.03	https://github.com/glkfc/IoT-Vulnerability/blob/main/TRENDnet/TRENDnet_TEW635BRM_ipoa_cmdinj_EN.md https://vuldb.com/cve/CVE-2026-15481 https://vuldb.com/submit/838237 https://vuldb.com/vuln/377788 https://vuldb.com/vuln/377788/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-15484	8,8	TRENDnet	Improper Restriction of Operations within the Bounds of a Memory Buffer	TRENDnet TEW-821DAP 1.12B01	https://github.com/IOTRes/IOT_Firmware_Update/blob/main/Trendnet/TEW-821DAP_BO3.md https://vuldb.com/cve/CVE-2026-15484 https://vuldb.com/submit/842381 https://vuldb.com/vuln/377791 https://vuldb.com/vuln/377791/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-15543	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CH22 1.0.0.1	https://candle-throne-f75.notion.site/Tenda-CH22-formCertListInfo-377df0aa11858088aabaeb0f5e1909c9 https://vuldb.com/cve/CVE-2026-15543 https://vuldb.com/submit/855077 https://vuldb.com/vuln/377893 https://vuldb.com/vuln/377893/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-49972	8,8	Laravel-Mediable	Unrestricted Upload of File with Dangerous Type	Laravel-Mediable before 7.0.0	https://github.com/plank/laravel-mediable/commit/49e3583bed13423611b3391f89e6b002571eed73 https://github.com/plank/laravel-mediable/releases/tag/7.0.0 https://www.vulncheck.com/advisories/laravel-mediable-file-upload-rce-via-extension-bypass
https://nvd.nist.gov/vuln/detail/CVE-2026-55773	8,8	CedarJava	Improper Control of Generation of Code ('Code Injection')	CedarJava is an open source Java implementation of the Cedar policy language, used for fine-grained authorization decisions. In versions prior to 2.3.6, 3.4.1 and 4.9.0	https://github.com/cedar-policy/cedar-java/security/advisories/GHSA-qmch-v2q9-wg4p
https://nvd.nist.gov/vuln/detail/CVE-2026-57856	8,8	Cockpit CMS	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Cockpit CMS	https://gist.github.com/sermikr0/821c4edd3c34e98a62a50b07707785bd https://github.com/Cockpit-HQ/Cockpit/commit/dde2d1d74f5f4e11de42a298918ea8c9684f932c https://github.com/cockpit-hq/cockpit https://www.vulncheck.com/advisories/cockpit-cms-missing-authorization-in-bucket-file-storage-api https://www.vulncheck.com/advisories/cockpit-cms-path-traversal-via-bucket-name-in-bucket-file-storage-api
https://nvd.nist.gov/vuln/detail/CVE-2026-62200	8,8	OpenClaw	Incomplete List of Disallowed Inputs	OpenClaw versions before 2026.6.1	https://github.com/openclaw/openclaw/security/advisories/GHSA-9969-8g9h-rxwm

					https://www.vulncheck.com/advisories/openclaw-authentication-bypass-via-git-ext-transport
https://nvd.nist.gov/vuln/detail/CVE-2026-62242	8,6	Spring Boot Admin Server	Server-Side Request Forgery (SSRF)	Spring Boot Admin Server before 4.1.2	https://github.com/codecentric/spring-boot-admin/commit/1f991ea013e46360b8f8fb63fe4ad20a9bf0d551 https://github.com/codecentric/spring-boot-admin/issues/5452 https://github.com/codecentric/spring-boot-admin/pull/5464 https://github.com/codecentric/spring-boot-admin/releases/tag/4.1.2 https://www.vulncheck.com/advisories/spring-boot-admin-server-ssrf-via-unauthenticated-instance-registration
https://nvd.nist.gov/vuln/detail/CVE-2026-0487	8,4	SAProuter on Microsoft Windows	Uncontrolled Search Path Element	SAProuter on Microsoft Windows	https://me.sap.com/notes/3692165 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2026-48364	8,2	ColdFusion	Uncontrolled Search Path Element	ColdFusion versions 2025.9, 2023.20 and earlier	https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
https://nvd.nist.gov/vuln/detail/CVE-2026-56259	8,2	Crawl4AI	Exposure of Sensitive Information to an Unauthorized Actor	Crawl4AI before 0.8.8	https://github.com/unclecode/crawl4ai/security/advisories/GHSA-f989-c77f-r2cq https://www.vulncheck.com/advisories/crawl4ai-llm-credential-exfiltration-via-base-url-and-environment-variable-resolution
https://nvd.nist.gov/vuln/detail/CVE-2026-58065	8,1	Apache Airflow Git	Key Exchange without Entity Authentication	apache-airflow-providers-git before 0.4.1	http://www.openwall.com/lists/oss-security/2026/07/13/3 https://github.com/apache/airflow/pull/69103 https://lists.apache.org/thread/fjmclngfksz2kp7llpcjxzdz568h0zhc
https://nvd.nist.gov/vuln/detail/CVE-2026-59245	8,1	Apache Airflow FAB	Improper Privilege Management	apache-airflow-providers-fab before 3.7.2	http://www.openwall.com/lists/oss-security/2026/07/13/4 https://github.com/apache/airflow/pull/69106 https://lists.apache.org/thread/70f37q3mwov1vm3zolrfxlzds278c78h
https://nvd.nist.gov/vuln/detail/CVE-2026-9492	7,8	GIGABYTE	Exposed IOCTL with Insufficient Access Control	The MBStorage DRAM lighting control module within Gigabyte Control Center (GCC) developed by GIGABYTE Technology has an Improper Access Control vulnerability.	https://www.twcert.org.tw/en/cp-139-11034-f7f2f-2.html https://www.twcert.org.tw/tw/cp-132-11033-97316-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-61458	7,5	PasswordPusher	Improper Restriction of Excessive Authentication Attempts	PasswordPusher before 2.9.2	https://github.com/pglombardo/PasswordPusher/security/advisories/GHSA-59w3-h5v2-c4xw https://www.vulncheck.com/advisories/passwordpusher-passphrase-brute-force-via-unthrottled-endpoint
https://nvd.nist.gov/vuln/detail/CVE-2026-61870	7,5	ImageMagick	Missing Release of Memory after Effective Lifetime	ImageMagick before 7.1.2-26	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-m596-67p7-69wh https://www.vulncheck.com/advisories/imagemagick-before-26-memory-leak-via-viff-encoder
https://nvd.nist.gov/vuln/detail/CVE-2026-15479	7,3	H3C NX15	Weak Password Recovery Mechanism for Forgotten Password	H3C NX15 V100R017	https://github.com/coconut652-7/IOT_Vul_Public/tree/main/H3C/NX15R017/pre_auth_pwd_change https://vuldb.com/cve/CVE-2026-15479 https://vuldb.com/submit/837069

					https://vuldb.com/vuln/377785 https://vuldb.com/vuln/377785/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-15482	**7,3**	Aster Telecom Azcall	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Aster Telecom Azcall 10/11	https://vuldb.com/cve/CVE-2026-15482 https://vuldb.com/submit/841457 https://vuldb.com/vuln/377789 https://vuldb.com/vuln/377789/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-61442	**7,1**	PraisonAI Platform (praisonai-platform)		PraisonAI Platform (praisonai-platform) before 0.1.9	https://github.com/MervinPraison/PraisonAI/commit/846568c7a5d8ce9e71e56e4c213f027c04909753 https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-c78w-2q4r-68r7 https://www.vulncheck.com/advisories/praisonai-platform-before-authorization-bypass-via-patch
https://nvd.nist.gov/vuln/detail/CVE-2026-62189	**7,1**	OpenClaw	Improper Link Resolution Before File Access ('Link Following')	OpenClaw versions before 2026.6.9	https://github.com/openclaw/openclaw/security/advisories/GHSA-m38g-vpwj-mpg9 https://www.vulncheck.com/advisories/openclaw-symlink-following-via-mirror-sync

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-2026-48939 iCagenda Unrestricted Upload of File with Dangerous Type Vulnerability ▪ CVE-2026-56291 Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability	https://www.cisa.gov/news-events/alerts/2026/07/10/cisa-adds-two-known-exploited-vulnerabilities-catalog
Improve Router Hygiene to Protect Against Russian State-Sponsored Targeting		https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-194a
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2008-4128 Cisco IOS Cross-Site Request Forgery Vulnerability	https://www.cisa.gov/news-events/alerts/2026/07/13/cisa-adds-one-known-exploited-vulnerability-catalog

News

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

Σύντομη περιγραφή / Τίτλος	URL
Telegram's t.me Domain Suspended, ServerHold Status Breaks Links Worldwide	https://cybersecuritynews.com/telegrams-t-me-domain-suspended/
NSA Urges Organizations to Disable Cisco Smart Install as Russian Hackers Target Routers	https://cybersecuritynews.com/nsa-disable-cisco-smart/
AI-Powered 'Intelligent Worm' Could Regenerate Exploits and Adapt to Defenses in Real Time	https://cybersecuritynews.com/ai-powered-intelligent-worm-could-regenerate-exploits/
iPhone and MacBook Forensics Investigation Exposes £113,000 Property Fraud Operation	https://cybersecuritynews.com/iphone-and-macbook-forensics-investigation/
Anthropic Extends Claude Fable 5 Access From July 12 to July 19	https://cybersecuritynews.com/anthropic-extends-claude-fable-5-access/
Microsoft Testing Copilot Feature That Shows What's Slowing Down Your Windows 11 PC	https://cybersecuritynews.com/microsoft-testing-copilot-feature-windows-11/
Cyber Security Newsletter and Bulletin Weekly – 16-Year-Old Linux, Ubiquiti Flaws, Accenture Breach, Android 17 Exploit +20 Stories	https://cybersecuritynews.com/cyber-security-news-bulletin-weekly-july/
Apple Sues OpenAI and Former Employees for Alleged Theft of Trade Secrets	https://cybersecuritynews.com/apple-sues-openai/
CISA Details "Lessons from a Cyber Incident" After AWS GovCloud Credentials Leak	https://cybersecuritynews.com/cisa-details-aws-credentials-leak/

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 Compromised jscrambler With 15,800+ Weekly Downloads to Attack Developers	https://cybersecuritynews.com/hackers-compromised-jscrambler/
SpaceX and Starlink X Account Reportedly Compromised to Push Fake Crypto Coins	https://cybersecuritynews.com/spacex-account-reportedly-compromised/
281 Popular VPN Apps from the Google Play Store Leak Sensitive Data, Transfer Data Unencrypted	https://cybersecuritynews.com/vpn-apps-from-the-google-play-leaks/

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
CISA Warns of Joomla Sites Running iCagenda or Balbooa Exploited in Attacks	https://cybersecuritynews.com/joomla-sites-running-icagenda-or-balbooa-exploited/
Critical WordPress Plugin Vulnerability Allows Attackers to Gain Full Control Over Website	https://cybersecuritynews.com/wordpress-plugin-vulnerability-miniorange/
One Misconfigured Python HTTP Server Exposed Three Active Campaigns from Attackers	https://cybersecuritynews.com/one-misconfigured-python-http-server-exposed/
Hackers Can Exploit Motorola MR2600 Firmware Update Process to Gain Code Execution	https://cybersecuritynews.com/hackers-exploit-motorola-mr2600-firmware-update/
Microsoft Teams on macOS Screen Sharing Bug Causing Blank Screens	https://cybersecuritynews.com/microsoft-teams-on-macos/
Dell BIOS Flaw Lets Attackers Recover Admin Passwords From SPI Flash in Milliseconds	https://cybersecuritynews.com/dell-bios-flaw-admin-passwords/

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
Debian 13 Released With Security Updates, Bug Fixes and Driver Updates	https://cybersecuritynews.com/debian-13-released-with-updates/

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
Chrome Extension Used by 1.6 Million Users Silently Included Data Exfiltration Capa-bilities	https://cybersecuritynews.com/chrome-extension-used-million-users-data-exfiltration/
New macOS Stealer Mimics Apple's Crash Report Framework to Steal Browser Cre-dentials	https://cybersecuritynews.com/macos-stealer-mimics-apples-crash-report/
Turla Hackers Exploit SharePoint Flaw to Access Thousands of French User Accounts	https://cybersecuritynews.com/turla-hackers-exploit-sharepoint-flaw/
Internet-Wide Scans Target MCP Servers, Claude Credentials, and Exposed AI Mod-els	https://cybersecuritynews.com/internet-wide-scans-target-mcp-servers-claude-credentials/
Hackers are Using Vibe-Coded PowerShell Script to Enumerate Active Directory Ac-counts	https://cybersecuritynews.com/vibe-coded-powershell-script-active-directory/
Armored Likho APT Uses AI-Generated Loaders to Deploy BusySnake Stealer Against Government Targets	https://cybersecuritynews.com/armored-likho-apt-uses-ai-generated-loaders/
SpyGlace Attacks Abuse Trusted Developer Services to Evade Network Detection	https://cybersecuritynews.com/spyglace-attacks-abuse-trusted-developer-services/
Hackers Weaponize Real Academic Event Materials to Infect Researchers With RokRAT	https://cybersecuritynews.com/hackers-weaponize-real-academic-event-materials/
New Ghostcommit Attack Hides Malicious Prompts in Images to Exploit AI Agents	https://cybersecuritynews.com/ghostcommit-attack-hides-prompts/
Forg365 Phishing Platform Using AI to Attack Microsoft 365 Accounts	https://cybersecuritynews.com/forg365-phishing-attack-microsoft-365-accounts/
Progress Urges ShareFile Admins to Shut Down Servers Over Credible Security Threat	https://cybersecuritynews.com/progress-sharefile-admins-shut-down-servers/

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 επαγ-γελματιών ασφάλειας.

Σύντομη περιγραφή / Τίτλος	URL
VEXAIoT Multi-Agent System Automates IoT Reconnaissance and Exploit Execution	https://cybersecuritynews.com/vexaiot-automates-iot-reconnaissance/
Citrix Unveils NetScaler MCP Gateway With Centralized Security for AI Agents	https://cybersecuritynews.com/citrix-unveils-netscaler-mcp-gateway/
KittySploit – AI-Powered Next-Generation Penetration Testing Framework With 1150+ Modules	https://cybersecuritynews.com/kittysploit-penetration-testing-tool/

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/