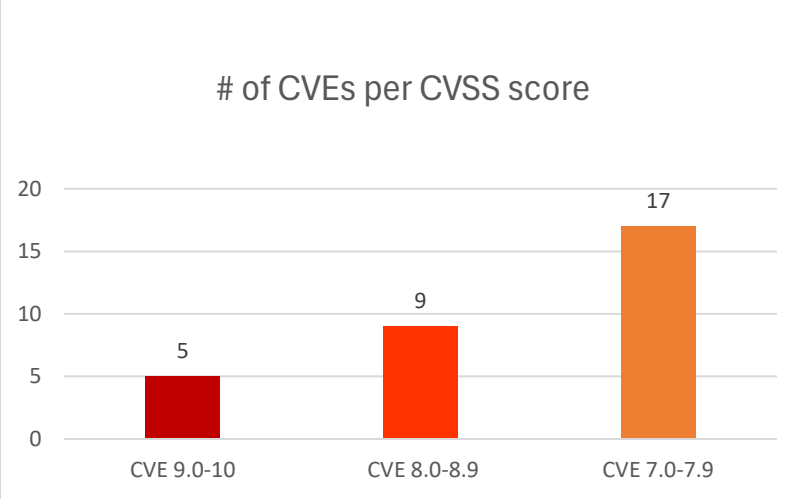
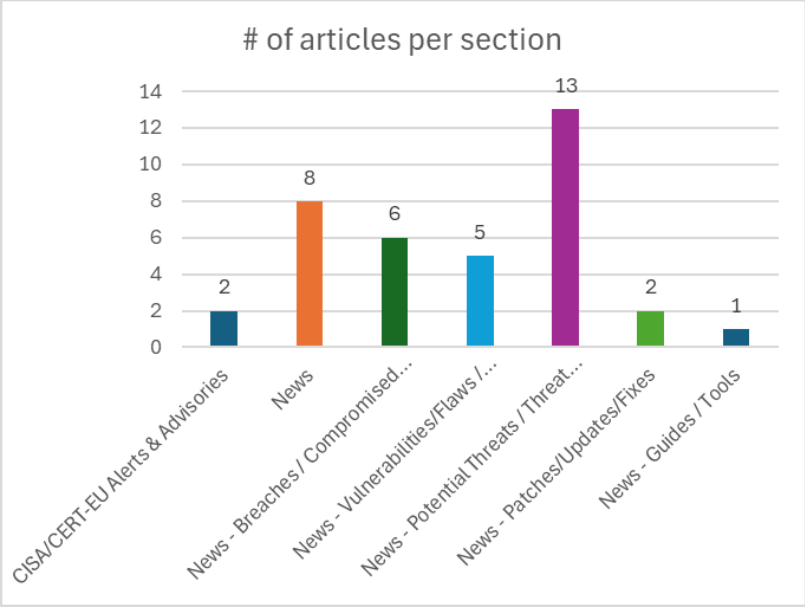
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 20/06/2026 - 23/06/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 6
News 6
Breaches / Compromised / Hacked 7
Vulnerabilities / Flaws / Zero-day 7
Patches / Updates / Fixes 8
Potential threats / Threat intelligence 8
Guides / Tools 9
References 10
Annex – Websites with vendor specific vulnerabilities 11

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 /Υπη-ρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-10561	10	IBM	Improper Control of Generation of Code ('Code Injection')	IBM Langflow OSS 1.0.0 through 1.9.3	https://www.ibm.com/support/pages/node/7277242
https://nvd.nist.gov/vuln/detail/CVE-2026-7664	9,8	IBM	Improper Authentication	IBM Langflow OSS 1.0.0 through 1.8.4	https://www.ibm.com/support/pages/node/7277243
https://nvd.nist.gov/vuln/detail/CVE-2026-10789	9,6	Autodesk	Improper Control of Generation of Code ('Code Injection')	Autodesk Fusion Desktop	https://dl.appstreaming.autodesk.com/production/installers/Fusion%20Client%20Downloader.dmg https://dl.appstreaming.autodesk.com/production/installers/Fusion%20Client%20Downloader.exe https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0008
https://nvd.nist.gov/vuln/detail/CVE-2026-28381	9,6	Grafana Labs	-	Snowflake Datasource	https://grafana.com/security/security-advisories/cve-2026-28381
https://nvd.nist.gov/vuln/detail/CVE-2026-48746	9,1	ASGI web servers	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	vLLM is an inference and serving engine for large language models (LLMs). From 0.3.0 until 0.22.0	https://github.com/vllm-project/vllm/pull/43426 https://github.com/vllm-project/vllm/security/advisories/GHSA-94f4-hr76-p5j6 https://x41-dsec.de/lab/advisories/x41-2026-002-starlette
https://nvd.nist.gov/vuln/detail/CVE-2026-12806	8,8	Edimax	Improper Restriction of Operations within the Bounds of a Memory Buffer	Edimax BR-6478AC V2 1.23	https://lavender-bicycle-a5a.notion.site/EDIMAX-BR6478ACV2-formWlSiteSurvey-34b53a41781f80669c10df409a0851d4?source=copy_link https://vuldb.com/cve/CVE-2026-12806 https://vuldb.com/submit/836668 https://vuldb.com/vuln/372600 https://vuldb.com/vuln/372600/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-44272	8,8	Dell	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Dell Wyse Management Suite (WMS), versions prior to WMS 2605	https://www.dell.com/support/kbdoc/en-us/000472001/dsa-2026-247
https://nvd.nist.gov/vuln/detail/CVE-2026-54099	8,8	Red Hat, Inc.	Improper Privilege Management	Windows Machine Config Operator (WMCO) for Red Hat OpenShift Container Platform	https://access.redhat.com/security/cve/CVE-2026-54099 https://bugzilla.redhat.com/show_bug.cgi?id=2487950
https://nvd.nist.gov/vuln/detail/CVE-2026-56266	8,6	Crawl4AI	Server-Side Request Forgery (SSRF)	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-server-side-request-forgery-via-direct-crawl-endpoints
https://nvd.nist.gov/vuln/detail/CVE-2026-54100	8,3	Red Hat, Inc.	Improper Certificate Validation	Windows Machine Config Operator (WMCO) for Red Hat OpenShift Container Platform	https://access.redhat.com/security/cve/CVE-2026-54100 https://bugzilla.redhat.com/show_bug.cgi?id=2487953
https://nvd.nist.gov/vuln/detail/CVE-2025-66336	8,1	Apache Doris	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Apache Doris MCP Server	http://www.openwall.com/lists/oss-security/2026/06/22/1 https://lists.apache.org/thread/4l4v3m7ofwrgp4s4s98pjb5l03fcrzo2
https://nvd.nist.gov/vuln/detail/CVE-2026-12628	8,1	IBM	Use of Hard-coded Credentials	IBM Storage Protect Client 8.1.0.0 through 8.2.1.0 and IBM Storage Protect Snapshot For Windows 8.1.0.0 through 8.2.1.0	https://www.ibm.com/support/pages/node/7277245
https://nvd.nist.gov/vuln/detail/CVE-2026-56345	8,1	AVideo	Improper Authentication	AVideo through 29.0	https://github.com/WWBN/AVideo/security/advisories/GHSA-qxvm-r42f-5p8j https://www.vulncheck.com/advisories/avideo-arbitrary-user-session-hijacking-via-meet-plugin-uploadrecordedvideo-endpoint
https://nvd.nist.gov/vuln/detail/CVE-2026-9072	8,1	IBM	Improper Control of Generation of Code ('Code Injection')	IBM i 7.6, 7.5, 7.4, and 7.3, IBM WebSphere Application Server, and IBM WebSphere Application Server Liberty	https://www.ibm.com/support/pages/node/7277344
https://nvd.nist.gov/vuln/detail/CVE-2026-12779	7,8	AOMEI	Incorrect Privilege Assignment	AOMEI Dynamic Disk Manager up to 10.10.1	https://vuldb.com/cve/CVE-2026-12779 https://vuldb.com/submit/835608 https://vuldb.com/vuln/372520 https://vuldb.com/vuln/372520/cti https://winslow1984.com/books/cve-collection/page/aomei-dynamic-disk-manager-10101-kernel-driver-ddmdrvsys-local-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2026-12780	7,8	AOMEI	Incorrect Privilege Assignment	AOMEI Backupper up to 8.3.0	https://vuldb.com/cve/CVE-2026-12780 https://vuldb.com/submit/835609 https://vuldb.com/vuln/372521 https://vuldb.com/vuln/372521/cti https://winslow1984.com/books/cve-collection/page/aomei-backupper-830-kernel-driver-amwrtdrvsys-local-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2026-12782	7,8	EaseUS	Incorrect Privilege Assignment	EaseUS Partition Master up to 14.5	https://vuldb.com/cve/CVE-2026-12782 https://vuldb.com/submit/835612 https://vuldb.com/vuln/372523 https://vuldb.com/vuln/372523/cti V https://winslow1984.com/books/cve-collection/page/easeus-partition-master-145-kernel-driver-euedkepmsys-local-privilege-escalation https://www.easeus.com/partition-manager/
https://nvd.nist.gov/vuln/detail/CVE-2026-12784	7,8	IM-Magic	Incorrect Privilege Assignment	IM-Magic Partition Resizer up to 7.9.0	https://vuldb.com/cve/CVE-2026-12784 https://vuldb.com/submit/835613 https://vuldb.com/vuln/372524 https://vuldb.com/vuln/372524/cti https://winslow1984.com/books/cve-collection/page/im-magic-partition-resizer-790-kernel-driver-mda-ntdrvsys-local-privilege-escalation

https://nvd.nist.gov/vuln/detail/CVE-2026-12786	7,8	Ezbsystems	Incorrect Privilege Assignment	Ezbsystems UltraISO Premium Edition up to 9.76	https://vuldb.com/cve/CVE-2026-12786 https://vuldb.com/submit/835614 https://vuldb.com/vuln/372528 https://vuldb.com/vuln/372528/cti https://winslow1984.com/books/cve-collection/page/ultraiso-premium-976-kernel-driver-bootpt64sys-local-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2026-44274	7,8	Dell	Improper Link Resolution Before File Access ('Link Following')	Dell Wyse Management Suite (WMS), versions prior to WMS 2605	https://www.dell.com/support/kbdoc/en-us/000472001/dsa-2026-247
https://nvd.nist.gov/vuln/detail/CVE-2026-42129	7,7	Loki	-	-	https://grafana.com/security/security-advisories/cve-2026-42129
https://nvd.nist.gov/vuln/detail/CVE-2025-66389	7,5	GitHub Copilot	Files or Directories Accessible to External Parties	GitHub Copilot 1.372.0	https://blindcyber.com/2025/10/28/copilot-fun/ https://github.com/microsoft/vscode-copilot-chat/ https://github.com/microsoft/vscode/blob/03baef1008086ed4960042fa463e570072173bb5/src/vs/workbench/contrib/chat/electron-browser/tools/fetchPageTool.ts#L152
https://nvd.nist.gov/vuln/detail/CVE-2026-48506	7,5	C#	Uncontrolled Recursion	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7	https://github.com/MessagePack-CSharp/MessagePack-CSharp/security/advisories/GHSA-vh6j-jc39-fggf
https://nvd.nist.gov/vuln/detail/CVE-2026-53539	7,5	Python	Uncontrolled Resource Consumption	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.30	https://github.com/Kludex/python-multipart/security/advisories/GHSA-5rvq-cxj2-64vf
https://nvd.nist.gov/vuln/detail/CVE-2026-8858	7,5	IBM	Improper Control of Generation of Code ('Code Injection')	IBM i 7.6, 7.5, 7.4, and 7.3, IBM WebSphere Application Server and IBM WebSphere Application Server Liberty	https://www.ibm.com/support/pages/node/7277344
https://nvd.nist.gov/vuln/detail/CVE-2026-9071	7,5	IBM	Uncontrolled Resource Consumption	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6	https://www.ibm.com/support/pages/node/7276579
https://nvd.nist.gov/vuln/detail/CVE-2026-8646	7,4	IBM	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	IBM WebSphere Application Server 9.0 and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6	https://www.ibm.com/support/pages/node/7276579
https://nvd.nist.gov/vuln/detail/CVE-2026-9006	7,4	IBM	Server-Side Request Forgery (SSRF)	IBM WebSphere Application Server 9.0, and 8.5	https://www.ibm.com/support/pages/node/7276600
https://nvd.nist.gov/vuln/detail/CVE-2026-10845	7,3	IBM	Improper Authentication	IBM WebSphere Application Server 8.5 and 9.0	https://www.ibm.com/support/pages/node/7276597
https://nvd.nist.gov/vuln/detail/CVE-2026-9029	7,3	Grafana Labs	-	geomap panel's XYZ tile layer	https://grafana.com/security/security-advisories/cve-2026-9029
https://nvd.nist.gov/vuln/detail/CVE-2026-56382	7,2	Craft CMS	Improper Control of Generation of Code ('Code Injection')	Craft CMS (composer package craftcms/cms) versions >= 5.5.0 and <= 5.9.13	https://github.com/craftcms/cms/security/advisories/GHSA-86vw-x4ww-x467 https://www.vulncheck.com/advisories/craft-cms-remote-code-execution-via-missing-config-sanitization-in-fieldscontroller

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-2026-20253 Splunk Enterprise Missing Authentication for Critical Function Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure		https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-urges-hardening-fortinet-devices-after-reports-credential-exposure

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
Researcher Earns $148,337 for Google Cloud Production RCE Vulnerability	https://cybersecuritynews.com/google-cloud-production-rce-vulnerability/
OpenAI Releases GPT-5.5-Cyber With Full Automation for Vulnerability Detection and Patching	https://cybersecuritynews.com/gpt-5-5-cyber/
29-Year-Old ‘Squidbleed’ Vulnerability Discovered With the Aid of Claude Mythos Preview	https://cybersecuritynews.com/squidbleed-vulnerability/
Microsoft’s New Option Allows Organizations to Block Copilot Access to Office Files	https://cybersecuritynews.com/microsoft-copilot-block-office-files/
Microsoft has urged IT Admins to Prepare for Windows 11, Version 26H2 Update	https://cybersecuritynews.com/microsoft-urged-windows-11-26h2-update/
13-Word Reddit Comment Can Poison ChatGPT and Gemini AI Search Results	https://cybersecuritynews.com/13-word-reddit-comment-chatgpt-and-gemini/
Anthropic’s Claude AI Back Online After 90-Minute Global Outage	https://cybersecuritynews.com/anthropic-claude-ai-outage/
FortiBleed – Fortinet Warns of Active Credential Harvesting Campaign Targeting FortiGate Devices	https://cybersecuritynews.com/fortibleed-credential-harvesting-attack/

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
Tata Electronics Data Breach Exposes Confidential Apple and Tesla Documents	https://cybersecuritynews.com/tata-electronics-data-breach/
AryStinger Botnet Hijacks 4,300+ Routers to Build Global Attack Proxy Network	https://cybersecuritynews.com/arystinger-botnet-hijacks-4300-routers/
Klue Hack Leads to Data Breach Across Multiple Cybersecurity Companies	https://cybersecuritynews.com/klue-hack-cybersecurity-companies/
North Korean Hackers Abuse Mastra npm Supply Chain to Target Developers and CI/CD Pipelines	https://cybersecuritynews.com/north-korean-hackers-abuse-mastra-npm-supply-chain/
Hackers Compromised 10,000+ GitHub Repositories to Inject Malicious Script	https://cybersecuritynews.com/hackers-github-malicious-script/
Anthropic's Mythos AI Model Reportedly Breached NSA Classified Systems in Hours	https://cybersecuritynews.com/anthropics-mythos-ai-model/

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 libssh2 Vulnerability Allows Attackers to Execute Remote Code Via Malicious SSH packets	https://cybersecuritynews.com/libssh2-vulnerability/
Critical FFmpeg Vulnerability Allows Attackers to Weaponize Media Files	https://cybersecuritynews.com/ffmpeg-vulnerability-weaponize-media-files/
Microsoft Entra Conditional Access Policies Can Be Bypassed Via Nested App Authentication	https://cybersecuritynews.com/microsoft-entra-access-policies-nested-app/
Apple Beats Studio Buds Vulnerability Allows Hackers to Eavesdrop on Users	https://cybersecuritynews.com/apple-beats-studio-buds-vulnerability/
GentleKiller Ransomware Abuses Vulnerable Drivers to Disable 400+ EDR Security Processes	https://cybersecuritynews.com/gentlekiller-ransomware-edr-processes/

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
pgAdmin 4 Released With Fixes for Seven Security Vulnerabilities and New Features	https://cybersecuritynews.com/pgadmin-4-released/
QNAP Patches Multiple Injection Vulnerabilities Leads to Arbitrary Command Execution	https://cybersecuritynews.com/qnap-patches-multiple-injection-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 Phishing Attack Abuses Outlook and Microsoft 365 Groups Features to Attack Users	https://cybersecuritynews.com/new-phishing-attack-abuses-outlook-and-microsoft-365-groups/
Hackers Using FortigateSniffer Tool That Turns Compromised Firewalls Into Password Collectors	https://cybersecuritynews.com/fortigatesniffer-tool-fortibleed/
23 ClawHub Plugins Abuse Official Org Scopes to Impersonate Trusted AI Agent Tools	https://cybersecuritynews.com/23-clawhub-plugins-abuse-official-org-scopes/
Windows RAT Uses Encrypted HTTP C2 and Registry Persistence After npm Infection	https://cybersecuritynews.com/windows-rat-uses-encrypted-http-c2/
Malicious GST Debit Note Attachment Deploys Remcos RAT Through Multi-Stage Loader	https://cybersecuritynews.com/malicious-gst-debit-note-attachment-deploys-remcos-rat/
AI-Powered iOS Apps Leaking LLM API Credentials Through Network Traffic	https://cybersecuritynews.com/ai-ios-apps-leaking-llm-credentials/
Hackers Use RemotePC RMM and PowerShell Stagers to Deploy Prinz Eugen Ransomware	https://cybersecuritynews.com/hackers-use-remotepc-rmm-and-powershell-stagers/
New Malware Attack Via WhatsApp Attacking Windows System to Enable Remote Access For Attackers	https://cybersecuritynews.com/new-malware-attack-via-whatsapp-attacking-windows-system/
GitHub Actions Checkout Update Blocks Workflows Triggered by Malicious pull_request_target	https://cybersecuritynews.com/github-actions-checkout-update-workflow/
Chinese Cyber Contractors Use Malware, Botnets, and Stolen Data to Enable State Operations	https://cybersecuritynews.com/chinese-cyber-contractors-use-malware-botnets-and-stolen-data/
Hackers Impersonate Node.js Installer in Google Ads to Deploy Infostealer Malware	https://cybersecuritynews.com/hackers-impersonate-node-js-installer-in-google-ads/
Malicious JetBrains and VS Code Extensions Steal OpenAI, Anthropic, and DeepSeek API Keys	https://cybersecuritynews.com/malicious-jetbrains-and-vs-code-extensions-steal-api-keys/
AutoJack – A Single Web Page Can Hijack Your AI Agent to Execute Malicious Code	https://cybersecuritynews.com/autojack/

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
CyberSentinel AI with 33 Security Tools, Including Nmap, SQLMap, ZAP, and uses Claude, GPT	https://cybersecuritynews.com/cybersentinel-ai-with-33-security-tools/

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/