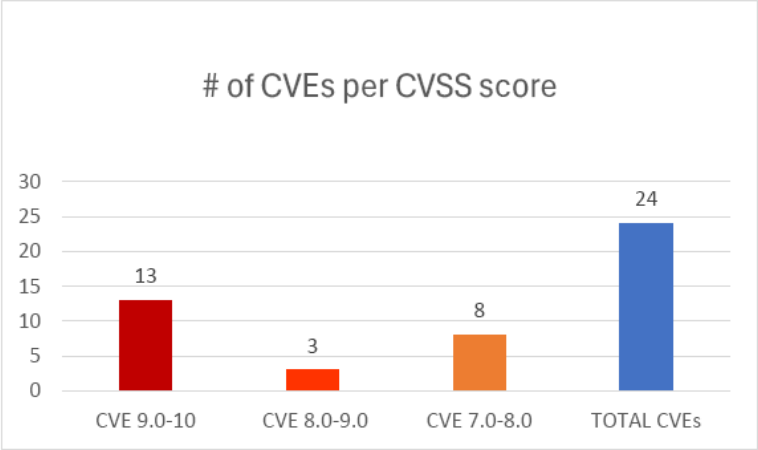
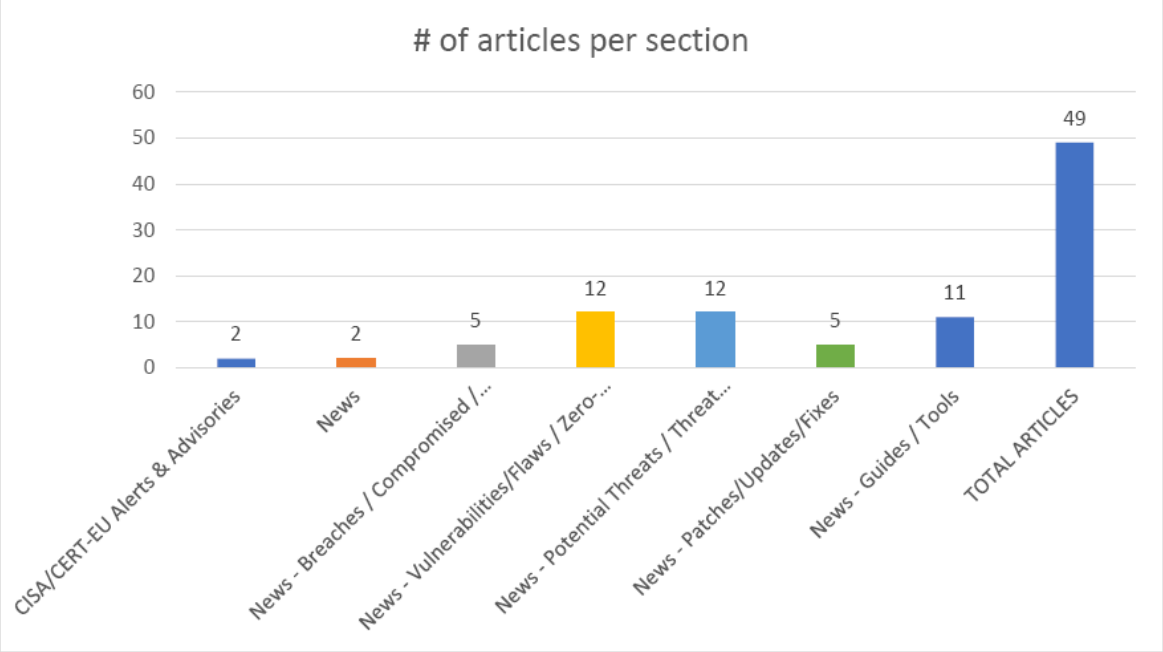
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 06/05/2026 - 08/05/2026





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)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-7854	9,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	DI-8100 16.07.26A1	https://github.com/draw-ctf/report/blob/main/DI-8100/url_rule_asp_overflow.md VulDB Exploit Third Party Advisory https://vuldb.com/submit/807838 VulDB Third Party Advisory VDB Entry https://vuldb.com/vuln/361131 VulDB Third Party Advisory https://vuldb.com/vuln/361131/cti VulDB Permissions Required VDB Entry https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-7414	9,8	Yarbo firmware	Use of Hard-coded Credentials	v2.3.9	https://github.com/Bin4ry/yarbo-nat-in-my-back-yard
https://nvd.nist.gov/vuln/detail/CVE-2026-7690	9,8	Wavlink	Improper Neutralization of Special Elements in Output Used by a Down-stream Component ('In-jection')	WL-WN570HA1 R70HA1 V1410_221110	https://lavender-bicycle-a5a.notion.site/Wavlink-WN570HA1-set_sys_adm-34753a41781f809d8043f0a7a3e07e50?source=copy_link VulDB Exploit Third Party Advisory https://vuldb.com/submit/807805 VulDB Third Party Advisory VDB Entry https://vuldb.com/vuln/360860 VulDB Third Party Advisory VDB Entry https://vuldb.com/vuln/360860/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-42027	9,8	Arbitrary Class In-stantiation	Use of Externally-Controlled Input to Select Classes or	before 2.5.9, before 3.0.0-M3	http://www.openwall.com/lists/oss-security/2026/05/01/20 CVE Mailing List Third Party Advisory https://lists.apache.org/thread/ltlo4pow-jfc0w2w2yyl1o5tc7q1gcb2y

		via Model Manifest	Code ('Unsafe Reflection')		
https://nvd.nist.gov/vuln/detail/CVE-2026-42235	9,8	n8n	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to versions 1.123.32, 2.17.4, and 2.18.1	https://github.com/n8n-io/n8n/security/advisories/GHSA-537j-gqpc-p7fq
https://nvd.nist.gov/vuln/detail/CVE-2026-42238	9,8	Nginx UI	Improper Control of Generation of Code ('Code Injection')	Prior to version 2.3.8	https://github.com/0xJacky/nginx-ui/releases/tag/v2.3.8 GitHub, Inc. Release Notes https://github.com/0xJacky/nginx-ui/security/advisories/GHSA-4pvg-prr3-9cxr
https://nvd.nist.gov/vuln/detail/CVE-2026-42284	9,8	GitPython	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	Prior to version 3.1.47	https://github.com/gitpython-developers/GitPython/releases/tag/3.1.47 GitHub, Inc. Patch Release Notes https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-x2qx-6953-8485
https://nvd.nist.gov/vuln/detail/CVE-2026-7910	9,6	Views in Google Chrome	Use After Free	prior to 148.0.7778.96	https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html Chrome Vendor Advisory https://issues.chromium.org/issues/497543810
https://nvd.nist.gov/vuln/detail/CVE-2026-42880	9,6	Argo CD	Exposure of Sensitive Information to an Unauthorized Actor	From versions 3.2.0 to before 3.2.11 and 3.3.0 to before 3.3.9	https://github.com/argoproj/argo-cd/security/advisories/GHSA-3v3m-wc6v-x4x3
https://nvd.nist.gov/vuln/detail/CVE-2026-7821	9,1	Ivanti EPMM	Improper Certificate 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
https://nvd.nist.gov/vuln/deta	9,1	Plack::Middleware::Xsendfile	Improper Control of Dynamically-Managed Code Resources	through 1.0053	https://metacpan.org/release/MIYAGAWA/Plack-1.0053/changes CPANSec Release Notes https://metacpan.org/release/MIYAGAWA/Plack-

il/CVE-2026-7381					1.0053/view/lib/Plack/Middleware/XSendfile.pm#DEPRECATION-NOTICE CPANSec Product https://nvd.nist.gov/vuln/detail/CVE-2025-61780
https://nvd.nist.gov/vuln/detail/CVE-2026-43578	9,1	OpenClaw	Incomplete List of Disallowed Inputs	2026.3.31 before 2026.4.10	https://github.com/openclaw/openclaw/commit/19a2e9ddb5a8a494abcba812bb11f51075026a27 VulnCheck Patch https://github.com/openclaw/openclaw/security/advisories/GHSA-g375-h3v6-4873 VulnCheck Mitigation Vendor Advisory https://www.vulncheck.com/advisories/openclaw-privilege-escalation-via-missed-async-exec-completion-events-in-heartbeat-owner-downgrade
https://nvd.nist.gov/vuln/detail/CVE-2026-44597	9,1	Tor	Incorrect Provision of Specified Functionality	before 0.4.9.7	https://forum.torproject.org/c/news/tor-release-announcement/28 MITRE Release Notes https://gitlab.torproject.org/tpo/core/tor/-/commit/8f98054b1982d00a14639864d03e9afd90b87481 MITRE Patch https://gitlab.torproject.org/tpo/core/tor/-/work_items/41254 MITRE Broken Link https://www.openwall.com/lists/oss-security/2026/05/06/8
https://nvd.nist.gov/vuln/detail/CVE-2026-8138	8,8	Tenda	Stack-based Buffer Overflow	CX12L 16.03.53.12	https://github.com/cve-a/lvdan/issues/6 VulDB https://vuldb.com/submit/808867 VulDB https://vuldb.com/vuln/361927 VulDB https://vuldb.com/vuln/361927/cti VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-6819	8,8	HKUDS OpenHarness	Incorrect Default Permissions	prior to PR #156	https://github.com/HKUDS/OpenHarness/commit/59017e09880fcf9a6f60456a84fb982900b2c0b2 VulnCheck Patch https://github.com/HKUDS/OpenHarness/pull/156 CISA-ADP, VulnCheck Exploit Issue Tracking Patch https://github.com/HKUDS/OpenHarness/releases/tag/v0.1.7 VulnCheck Release Notes

					https://www.vulncheck.com/advisories/hkuds-openharness-plugin-management-command-exposure
https://nvd.nist.gov/vuln/detail/CVE-2026-8018	8,1	DevTools in Google Chrome	Insufficient Information	prior to 148.0.7778.96	https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html Chrome Release Notes Vendor Advisory https://issues.chromium.org/issues/498292657
https://nvd.nist.gov/vuln/detail/CVE-2026-7736	7,5	osrg GoBGP	Integer Underflow (Wrap or Wraparound)	up to 4.3.0	https://github.com/osrg/gobgp/ VulDB Product https://github.com/osrg/gobgp/commit/76d911046344a3923cbe573364197aa081944592 VulDB Patch https://github.com/osrg/gobgp/releases/tag/v4.4.0 VulDB Patch Product https://vuldb.com/submit/807604 VulDB Third Party Advisory VDB Entry https://vuldb.com/vuln/360911 VulDB Third Party Advisory VDB Entry https://vuldb.com/vuln/360911/cti
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')	719.v80e905ef14eb_ and earlier	https://www.jenkins.io/security/advisory/2026-04-29/#SECURITY-3672
https://nvd.nist.gov/vuln/detail/CVE-2026-40436	7,5	The ZTE ZXEDM iEMS	Insufficient Information		https://support.zte.com.cn/zte-iccp-isupport-webui/support/bulletin/security?lang=en_US&t=0.7465962531829456
https://nvd.nist.gov/vuln/detail/CVE-2026-8133	7,3	zyx0814 FilePress	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	up to 2.2.0	https://github.com/xiaohaiyang-ai/Web-Security-Research/tree/main/FilePress/Shares-API-PreAuth-SQLi VulDB https://github.com/zyx0814/FilePress/ VulDB https://github.com/zyx0814/FilePress/commit/e20ec58414103f781858f2951d178e19b1736664 VulDB https://github.com/zyx0814/FilePress/issues/70 VulDB https://github.com/zyx0814/FilePress/pull/71 VulDB

					https://vuldb.com/submit/808819 VulDB https://vuldb.com/vuln/361923 VulDB https://vuldb.com/vuln/361923/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-8132	7,3	CodeAstro Leave Management System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://codeastro.com/ VulDB https://github.com/yihaofuweng/cve/issues/64 VulDB https://vuldb.com/submit/808784 VulDB https://vuldb.com/vuln/361922 VulDB https://vuldb.com/vuln/361922/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-43869	7,3	Apache Thrift	Improper Validation of Certificate with Host Mismatch	before 0.23.0	http://www.openwall.com/lists/oss-security/2026/05/05/3 CVE Mailing List Third Party Advisory https://lists.apache.org/thread/3hsgl1b69wzq3ry39scqbv2dhyl3j52r
https://nvd.nist.gov/vuln/detail/CVE-2026-6411	7,3	MAXHUB Pivot client application	Use of a Broken or Risky Cryptographic Algorithm	prior to v1.36.2	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-127-01.json ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-26-127-01 ICS-CERT https://www.maxhub.com/en/support/
https://nvd.nist.gov/vuln/detail/CVE-2026-41641	7,2	NocoBase	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Prior to version 2.0.39	https://github.com/nocobase/nocobase/commit/851aee543efa894142e0f7be03eb55d9cec06a91 GitHub, Inc. Patch https://github.com/nocobase/nocobase/pull/9134 GitHub, Inc. Issue Tracking Patch https://github.com/nocobase/nocobase/releases/tag/v2.0.39 GitHub, Inc. Patch Product https://github.com/nocobase/nocobase/security/advisories/GHSA-wrwh-c28m-9jjh

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-2026-0300 Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability	https://www.cisa.gov/news-events/alerts/2026/05/06/cisa-adds-one-known-exploited-vulnerability-catalog
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

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
From Prompts to Production: The Technical Guide to Secure Vibe Coding	https://thehackernews.uk/wiz-secure-coding
CISA Urges Critical Infrastructure Providers to Make Plans to Remain Operational if hit by Cyber-Attack	https://www.infosecurity-magazine.com/news/cisa-ci-fortify-isolation-recovery/

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
Critical Ollama Memory Leak Vulnerability Exposes 300,000 Servers Globally	https://cybersecuritynews.com/ollama-vulnerability-exposes-servers/
Massive 2.45B-Request DDoS Attack Used 1.2 Million IPs to Evade Rate Limits	https://cybersecuritynews.com/massive-2-45b-request-ddos-attack/
Azure AD Conditional Access Bypassed Via Phantom Device Registration and PRT Abuse	https://cybersecuritynews.com/azure-ad-conditional-access-bypassed/
Vimeo Data Breach Exposes 119,000 Users Unique Email Addresses	https://cybersecuritynews.com/vimeo-data-breach-exposed/
Zero-Auth Flaw Exposes DoD Contractor to Cross-Tenant Data Access	https://cybersecuritynews.com/zero-auth-flaw-exposes-dod-contractor/

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
vm2 Node.js Library Vulnerabilities Enable Sandbox Escape and Arbitrary Code Execution	https://thehackernews.com/2026/05/vm2-nodejs-library-vulnerabilities.html
Palo Alto PAN-OS Flaw Under Active Exploitation Enables Remote Code Execution	https://thehackernews.com/2026/05/palo-alto-pan-os-flaw-under-active.html
Microsoft Teams for Android Allow Users to Join Third-Party Meetings via SIP	https://cybersecuritynews.com/microsoft-teams-android-sip/
Argo CD's ServerSideDiff Vulnerability Enables Kubernetes Secret Extraction	https://cybersecuritynews.com/argo-cds-serversidediff-vulnerability/
New MajorDoMo RCE Vulnerability Exposes Servers to Code Execution Attacks	https://cybersecuritynews.com/majordomo-rce-vulnerability/
New Fanwei E-cology10 Server Vulnerability Could Let Attackers Hijack Sessions and Steal Credentials	https://cybersecuritynews.com/new-fanwei-e-cology10-server-vulnerability/
Salesforce Marketing Cloud Vulnerability Opened Door to Email Data Exposure	https://cybersecuritynews.com/salesforce-marketing-cloud-vulnerability/
Dirty Frag Linux Vulnerability Let Attackers Gain Root Privileges – PoC Released	https://cybersecuritynews.com/dirty-frag-linux-vulnerability/
New Ivanti EPMM 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/ivanti-epmm-0-day-exploited/
New Cisco Network Vulnerability Let Remote Attacker Cause DoS Attack	https://cybersecuritynews.com/cisco-network-vulnerability-dos-attack/
WatchGuard Agent Vulnerabilities Let Attackers Grant Full SYSTEM Privileges on Windows	https://cybersecuritynews.com/watchguard-agent-vulnerabilities-windows/
Critical Redis Vulnerabilities Enables Remote Code Execution Attacks	https://cybersecuritynews.com/redis-vulnerabilities-enables-rce/

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
Oracle Debuts Monthly Critical Security Patch Updates	https://www.securityweek.com/oracle-debuts-monthly-critical-security-patch-updates/
Palo Alto Networks to Patch Zero-Day Exploited to Hack Firewalls	https://www.securityweek.com/palo-alto-networks-to-patch-zero-day-exploited-to-hack-firewalls/
New Cisco DoS flaw requires manual reboot to revive devices	https://www.bleepingcomputer.com/news/security/new-cisco-dos-flaw-requires-manual-reboot-to-revive-devices/
Google Chrome 148 Released with Fix for 127 Security Vulnerabilities – Update Now	https://cybersecuritynews.com/chrome148-vulnerabilities-patched/
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. Περι-λαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Mirai-Based xlabs_v1 Botnet Exploits ADB to Hijack IoT Devices for DDoS Attacks	https://thehackernews.com/2026/05/mirai-based-xlabsv1-botnet-exploits-adb.html
CloudZ Malware Abuses Phone Link to Steal SMS OTPs	https://www.infosecurity-magazine.com/news/cloudz-rat-pheno-phone-link-otp/
Iran-Linked APT Posed as Chaos Ransomware Member in Espionage Campaign	https://www.infosecurity-magazine.com/news/iran-linked-apt-chaos-ransomware/
Hackers Used Claude AI to Attack on Water and Drainage Utility Systems	https://cybersecuritynews.com/hackers-used-claude-ai-to-attack/
New ClickFix Attack Targets macOS Users With Fake Disk Cleanup and Utility Lures	https://cybersecuritynews.com/new-clickfix-attack-targets-macos-users/
New Phishing Attack Weaponizing Event Invitations to Steal Login Credentials	https://cybersecuritynews.com/new-phishing-attack-weaponizing-event-invitations/
New Salat Malware Uses QUIC and WebSocket Channels for Stealthy Remote Con-trol	https://cybersecuritynews.com/new-salat-malware-uses-quic-and-websocket/
New FEMITBOT Network Uses Telegram Mini Apps to Push Crypto Fraud and An-droid Malware	https://cybersecuritynews.com/new-femitbot-network-uses-telegram-mini-apps/
QLNX Targets Developers With Credential Theft Designed for Supply Chain Com-promise	https://cybersecuritynews.com/qlnx-targets-developers-with-credential-theft/
Malicious OpenClaw DeepSeek Skill Exploits Agentic AI Workflows to Deliver RAT and Stealer	https://cybersecuritynews.com/malicious-openclaw-deepseek-skill-exploits-agentic-ai/
Iranian-Nexus Operation Targets Oman Ministries With Webshells, SQL Escalation, and Data Theft	https://cybersecuritynews.com/iranian-nexus-operation-targets-oman-ministries-with-webshells/
Ransomware and Data Extortion Groups Intensify Targeting of Aviation and Aero-space Sector	https://cybersecuritynews.com/ransomware-groups-intensify-targeting-of-aviation/

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
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
ThreatBook Launches Best-of-Breed Advanced Threat Intelligence Solution	https://cybersecuritynews.com/threatbook-advanced-threat-intelligence-solution/
CISA Releases Best Security Practices Guide for Hardening Microsoft Exchange Server	https://cybersecuritynews.com/microsoft-exchange-server-hardening-guide/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-management-tools/
NETREAPER Offensive Security Toolkit That Wraps 70+ Penetration Testing Tools	https://cybersecuritynews.com/netreaper-offensive-security-toolkit/
GitLab Security Best Practices Cheat Sheet	https://thehackernews.uk/gitlab-security-tips
False Negatives Are a New SOC Headache. Here's the Fast Way to Fix It	https://cybersecuritynews.com/false-negatives-are-a-new-soc-headache-heres-the-fast-way-to-fix-it/
PentAGI – Automated AI-Powered Penetration Testing Tool that Integrates 20+ Security Tools	https://cybersecuritynews.com/pentagi-penetration-testing-tool/
The CISO Executive Toolkit (Free Download)	https://thehackernews.uk/wiz-ciso-bundle
Secure Coding Best Practices: Practical Guide + Cheat Sheet for Developers	https://thehackernews.uk/secure-coding-wiz-cheat

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/