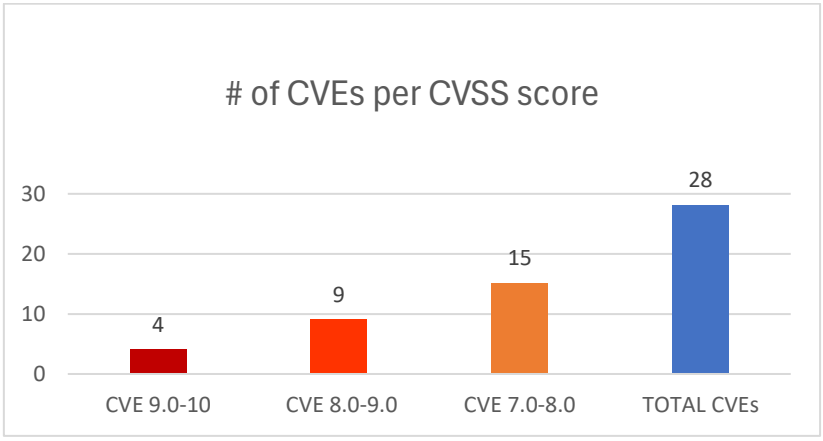
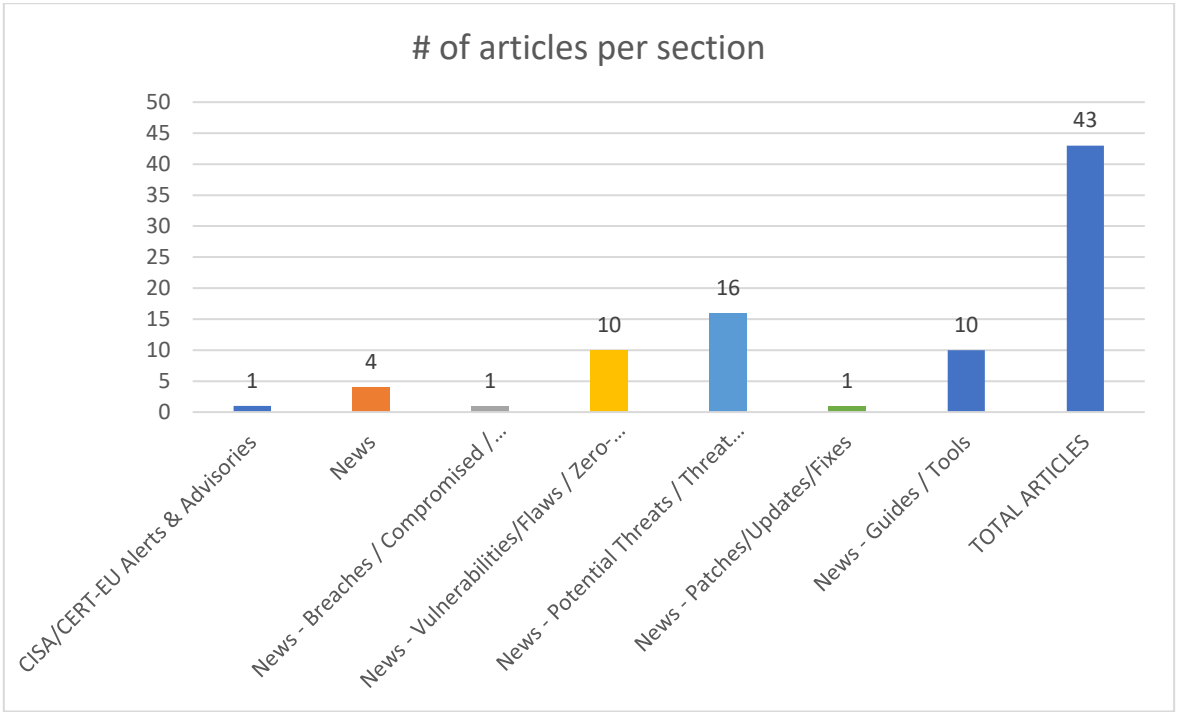
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 07/03/2026 - 10/03/2026





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-2026-30861	9,9	WeKnora	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	From version 0.2.5 to before version 0.2.10	https://github.com/Tencent/WeKnora/security/advisories/GHSA-r55h-3rwj-hcmg
https://nvd.nist.gov/vuln/detail/CVE-2026-3630	9,8	Delta Electronics COMMGR2	Stack-based Buffer Overflow		https://filecenter.deltaww.com/news/download/doc/Delta-PCSA-2026-00005_COMMGR%202%20Multiple%20Vulnerabilities%20(CVE-2026-3630,%20CVE-2026-3631).pdf
https://nvd.nist.gov/vuln/detail/CVE-2026-29191	9,3	ZITADEL	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	From version 4.0.0 to 4.11.1	https://github.com/zitadel/zitadel/security/advisories/GHSA-pr34-2v5x-6qjq
https://nvd.nist.gov/vuln/detail/CVE-2026-30832	9,1	Soft Serve	Server-Side Request Forgery (SSRF)	From version 0.6.0 to before version 0.11.4	https://github.com/charmbracelet/soft-serve/commit/3ef660098ab37a7950457da8ecc25b516e37ce4e GitHub, Inc. https://github.com/charmbracelet/soft-serve/releases/tag/v0.11.4 GitHub, Inc. https://github.com/charmbracelet/soft-serve/security/advisories/GHSA-3fvx-xrxq-8jvv
https://nvd.nist.gov/vuln/detail/CVE-2026-3823	8,8	EHG2408 series switch	Stack-based Buffer Overflow		https://www.twcert.org.tw/en/cp-139-10753-e091e-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10752-5a4d9-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-3810	8,8	Tenda FH1202	Improper Restriction of Operations within the Bounds of a Memory Buffer	1.2.0.14(408)	https://github.com/Svigo-o/Tenda_vul/tree/main/tenda-fh1202-dhcplistclient-page-buffer-overflow VulDB https://vuldb.com/?ctiid.349776 VulDB https://vuldb.com/?id.349776 VulDB https://vuldb.com/?submit.769040 VulDB https://www.tenda.com.cn/

https://nvd.nist.gov/vuln/detail/CVE-2026-3802	8,8	Tenda i3	Improper Restriction of Operations within the Bounds of a Memory Buffer	1.0.0.6(2204)	https://github.com/Svigo-o/Tenda_vul/tree/main/tenda-i3-formexeCommand-cmdinput-buffer-overflow VulDB https://vuldb.com/?ctiid.349769 VulDB https://vuldb.com/?id.349769 VulDB https://vuldb.com/?submit.768983 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-3715	8,8	Wavlink WL-WN579X3-C 231124	Improper Restriction of Operations within the Bounds of a Memory Buffer	-	https://dl.wavlink.com/firmware/RD/WN579X3C_WAVLINK_V20260226_WO_cb3003b2.bin VulDB https://github.com/Litengzheng/vul_db/blob/main/WL-WN579X3-C/vul_17/README.md VulDB https://vuldb.com/?ctiid.349660 VulDB https://vuldb.com/?id.349660 VulDB https://vuldb.com/?submit.765325
https://nvd.nist.gov/vuln/detail/CVE-2026-3698	8,8	UTT HiPER 810G	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 1.7.7-171114	https://github.com/7wkajk/CVE-VUL/blob/main/3.md VulDB https://vuldb.com/?ctiid.349644 VulDB https://vuldb.com/?id.349644 VulDB https://vuldb.com/?submit.765748
https://nvd.nist.gov/vuln/detail/CVE-2026-3701	8,8	H3C Magic B1	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 100R004	https://github.com/salted-fisholdxu/vul/blob/main/Magic%20B1/6_b1-report.md VulDB https://vuldb.com/?ctiid.349647 VulDB https://vuldb.com/?id.349647 VulDB https://vuldb.com/?submit.765771
https://nvd.nist.gov/vuln/detail/CVE-2026-30840	8,8	Wallos	Server-Side Request Forgery (SSRF)	Prior to version 4.6.2	https://github.com/ellite/Wallos/commit/e8a513591dbbf885966e2ef55c38622785b9060d GitHub, Inc. https://github.com/ellite/Wallos/releases/tag/v4.6.2 GitHub, Inc. https://github.com/ellite/Wallos/security/advisories/GHSA-mr2c-prqv-hqm8
https://nvd.nist.gov/vuln/detail/CVE-2026-30823	8,8	Flowise	Missing Authorization	Prior to version 3.0.13	https://github.com/FlowiseAI/Flowise/releases/tag/flowise%403.0.13 GitHub, Inc. https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-cwc3-p92j-g7qm

https://nvd.nist.gov/vuln/detail/CVE-2026-30851	8,1	Caddy	Insufficient Verification of Data Authenticity	From version 2.10.0 to before version 2.11.2	https://github.com/caddyserver/caddy/issues/6610 GitHub, Inc. https://github.com/caddyserver/caddy/pull/6608 GitHub, Inc. https://github.com/caddyserver/caddy/pull/7545 GitHub, Inc. https://github.com/caddyserver/caddy/security/advisories/GHSA-7r4p-vjf4-gxv4
https://nvd.nist.gov/vuln/detail/CVE-2026-30896	7,8	Qsee Client	Uncontrolled Search Path Element	1.0.1 and prior	https://jvn.jp/en/jp/JVN11676807/ JPCERT/CC https://www.q-see.com/pages/download
https://nvd.nist.gov/vuln/detail/CVE-2026-30929	7,7	ImageMagick	Out-of-bounds Write	Prior to versions 7.1.2-16 and 6.9.13-41	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-rqq8-jh93-f4vg
https://nvd.nist.gov/vuln/detail/CVE-2026-30827	7,5	express-rate-limit	Allocation of Resources Without Limits or Throttling	from 8.0.0 and prior to versions 8.0.2, 8.1.1, 8.2.2, and 8.3.0	https://github.com/express-rate-limit/express-rate-limit/commit/14e53888cdfd1b9798faf5b634c4206409e27fc4 GitHub, Inc. https://github.com/express-rate-limit/express-rate-limit/security/advisories/GHSA-46wh-pxpv-q5gq
https://nvd.nist.gov/vuln/detail/CVE-2026-29779	7,5	UptimeFlare	Exposure of Sensitive Information to an Unauthorized Actor	Prior to commit 377a596	https://github.com/lyc8503/UptimeFlare/commit/377a5963c66ba9a798abebfe8d80378b053435e9 GitHub, Inc. https://github.com/lyc8503/UptimeFlare/issues/198 GitHub, Inc. https://github.com/lyc8503/UptimeFlare/security/advisories/GHSA-36q9-v7p3-vj6v
https://nvd.nist.gov/vuln/detail/CVE-2026-3794	7,3	DoraCMS	Improper Authentication	3.0.x	https://vuldb.com/?ctiid.349761 VulDB https://vuldb.com/?id.349761 VulDB https://vuldb.com/?submit.768239
https://nvd.nist.gov/vuln/detail/CVE-2026-3765	7,3	University Management System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://github.com/mfcluvlife12345-eng/xianyu/issues/1 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.349743 VulDB https://vuldb.com/?id.349743 VulDB https://vuldb.com/?submit.768247
https://nvd.nist.gov/vuln/detail/CVE-2026-3764	7,3	SourceCodester Client Database Management System	Incorrect Privilege Assignment	1.0	https://gist.github.com/Adarshh-A/77dedc295e377e0492d15071e9bb2498 VulDB https://vuldb.com/?ctiid.349742 VulDB

					https://vuldb.com/?id.349742 VulDB https://vuldb.com/?submit.768195 VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-3759	7,3	Online Art Gallery Shop	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/hmKunlun/projectworldcve/issues/3 VulDB https://vuldb.com/?ctiid.349737 VulDB https://vuldb.com/?id.349737 VulDB https://vuldb.com/?submit.768059
https://nvd.nist.gov/vuln/detail/CVE-2026-3736	7,3	Simple Flight Ticket Booking System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/6Justdododo6/CVE/issues/12 VulDB https://vuldb.com/?ctiid.349714 VulDB https://vuldb.com/?id.349714 VulDB https://vuldb.com/?submit.768093
https://nvd.nist.gov/vuln/detail/CVE-2026-3730	7,3	Free Hotel Reservation System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/anon387tdug/anon387/issues/1 VulDB https://github.com/yihaofuweng/cve/issues/62 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.349708 VulDB https://vuldb.com/?id.349708 VulDB https://vuldb.com/?submit.767010 VulDB https://vuldb.com/?submit.767385
https://nvd.nist.gov/vuln/detail/CVE-2026-3696	7,3	Totolink N300RH	Improper Neutralization of Special Elements used in a Command ('Command Injection')	6..1c.1353_B20190305	https://github.com/JXBbozaihuang/vuln-research/issues/2 VulDB https://vuldb.com/?ctiid.349642 VulDB https://vuldb.com/?id.349642 VulDB https://vuldb.com/?submit.765681 VulDB https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-3693	7,3	Shy2593666979 AgentChat	Improper Control of Resource Identifiers ('Resource Injection')	up to 2.3.0	https://github.com/CC-T-454455/Vulnerabilities/tree/master/agent-chat/vulnerability-1 VulDB https://github.com/CC-T-454455/Vulnerabilities/tree/master/agent-chat/vulnerability-2 VulDB https://vuldb.com/?ctiid.349640 VulDB https://vuldb.com/?id.349640 VulDB https://vuldb.com/?submit.765589 VulDB https://vuldb.com/?submit.765590

https://nvd.nist.gov/vuln/detail/CVE-2026-29778	7,1	pyLoad	Relative Path Traversal	version 0.5.0b3.dev13 to 0.5.0b3.dev96	https://github.com/pyload/pyload/security/advisories/GHSA-6px9-j4qr-xfjw
https://nvd.nist.gov/vuln/detail/CVE-2026-30926	7,1	SiYuan	Improper Access Control	Prior to 3.5.10	https://github.com/siyuan-note/siyuan/security/advisories/GHSA-f9cq-v43p-v523
https://nvd.nist.gov/vuln/detail/CVE-2026-3787	7,0	UltraVNC	Uncontrolled Search Path Element	1.6.4.0	https://drive.google.com/file/d/14ixv_1i4D2VrZWyl4RKsvFcN1AMF_qNx/view VulDB https://vuldb.com/?ctiid.349754 VulDB https://vuldb.com/?id.349754 VulDB https://vuldb.com/?submit.767257

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 Three Known Exploited Vulnerabilities to Catalog	▪ **CVE-2021-22054 Omnissa Workspace ONE Server-Side Request Forgery** ▪ **CVE-2025-26399 SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability** ▪ **CVE-2026-1603 Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/03/09/cisa-adds-three-known-exploited-vulnerabilities-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
WiFi Signals Reveal Human Activities Through Walls by Mapping Body Keypoints	https://cybersecuritynews.com/wifi-signals-reveal-human-activities/
Google: Cloud attacks exploit flaws more than weak credentials	https://www.bleepingcomputer.com/news/security/google-cloud-attacks-exploit-flaws-more-than-weak-credentials/
iPhone Exploit Toolkit Used by Russian Spies Likely Originated from U.S. Contractor	https://cybersecuritynews.com/iphone-exploit-toolkit-and-russian-spies/
Microsoft Launches Copilot Cowork, a New AI Feature in Microsoft 365 to Automate Tasks	https://cybersecuritynews.com/copilot-cowork/

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
Cognizant TriZetto Data Breach Exposes Health Information of 3.4 Million Patients	https://cybersecuritynews.com/cognizant-trizetto-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
Anthropic Finds 22 Firefox Vulnerabilities Using Claude Opus 4.6 AI Model	https://thehackernews.com/2026/03/anthropic-finds-22-firefox.html
OpenAI Codex Security Scanned 1.2 Million Commits and Found 10,561 High-Severity Issues	https://thehackernews.com/2026/03/openai-codex-security-scanned-12.html
Recent Cisco Catalyst SD-WAN Vulnerability Now Widely Exploited	https://www.securityweek.com/recent-cisco-catalyst-sd-wan-vulnerability-now-widely-exploited/
CISA Warns of macOS and iOS Vulnerabilities Exploited in Attacks	https://cybersecuritynews.com/macos-and-ios-vulnerabilities-exploited/
Hackers Allegedly Selling Exploit for Windows Remote Desktop Services 0-Day Flaw	https://cybersecuritynews.com/windows-remote-desktop-services-0-day/
Critical Zero-Click Command Injection in AVideo Platform Allows Stream Hijacking	https://cybersecuritynews.com/avideo-platform-vulnerability/
CISA Flags SolarWinds, Ivanti, and Workspace One Vulnerabilities as Actively Exploited	https://thehackernews.com/2026/03/cisa-flags-solarwinds-ivanti-and.html
Apache ZooKeeper Vulnerability Allow Attackers to Access Sensitive Data	https://cybersecuritynews.com/apache-zookeeper-vulnerability/
Critical ExifTool Flaw Lets Malicious Images Trigger Code Execution on macOS	https://cybersecuritynews.com/critical-exiftool-flaw-lets-malicious-images/
Hikvision Multiple Products Vulnerability Allows Malicious Users to Escalate Privileges	https://cybersecuritynews.com/hikvision-multiple-products-vulnerability/

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
OpenAI Launches Codex Security that Discover, Validate and Patch Vulnerabilities	https://cybersecuritynews.com/openai-launches-codex-security/

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
When Auto-Updates Become Attack Paths	https://www.darkreading.com/endpoint-security/when-auto-updates-become-attack-paths
Malicious imToken Chrome Extension Caught Stealing Mnemonics and Private Keys	**https://cybersecuritynews.com/malicious-imtoken-chrome-extension/**
Threat Actor Exploits Flaws and Uses Elastic Cloud SIEM to Manage Stolen Data	https://www.infosecurity-magazine.com/news/elastic-cloud-siem-manage-stolen/
'InstallFix' Attacks Spread Fake Claude Code Sites	https://www.darkreading.com/cloud-security/installfix-attacks-fake-claude-code
Signed Malware Masquerading as Teams, Zoom Apps Drops RMM Backdoors	https://cybersecuritynews.com/signed-malware-masquerading-as-teams/
Chinese APT Campaign Targets Qatar With PlugX Lures Tied to Middle East Conflict	https://cybersecuritynews.com/chinese-apt-campaign-targets-qatar-with-plugx-lures/
GhostClaw Mimic as OpenClaw to Steal Everything from Developers	https://cybersecuritynews.com/ghostclaw-mimic-as-openclaw/
Hackers Attack Employees Over Microsoft Teams to Trick Them Into Granting Remote Access	https://cybersecuritynews.com/hackers-attack-over-microsoft-teams/
Hackers Use Fake CleanMyMac Site to Deploy SHub Stealer and Hijack Crypto Wallets	https://cybersecuritynews.com/hackers-use-fake-cleanmymac-site/
BoryptGrab Stealer Spreads via Fake GitHub Repositories, Stealing Browser and Crypto Wallet Data	https://cybersecuritynews.com/boryptgrab-stealer-spreads-via-fake-github-repositories/
MaaS VIP Keylogger Campaign Uses Steganography and In-Memory Execution to Steal Credentials at Scale	https://cybersecuritynews.com/maas-vip-keylogger-campaign-uses-steganography/
Vietnam-Based Cybercrime Network Enables Fraudulent Account Signups at Scale	https://cybersecuritynews.com/vietnam-based-cybercrime-network/
Iran-Linked Hackers Target U.S. Critical Infrastructure Amid Rising Cyber Threat Activity	https://cybersecuritynews.com/iran-linked-hackers-target-u-s-critical-infrastructure/
M365Pwned – Red Team GUI Toolkit for Microsoft 365 Exploitation via Graph API	https://cybersecuritynews.com/m365pwned-red-team-gui-toolkit/
ClipXDaemon Emerges as C2-Less Linux Clipboard Hijacker, Targeting Crypto Wallets in X11 Sessions	https://cybersecuritynews.com/clipxdaemon-emerges-as-clipboard-hijacker/
Microsoft Warns Fake AI Browser Extensions Compromised Chat Histories Across 20,000+ Enterprise Tenants	https://cybersecuritynews.com/microsoft-warns-fake-ai-browser-extensions-compromised-chat-histories/

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
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

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/