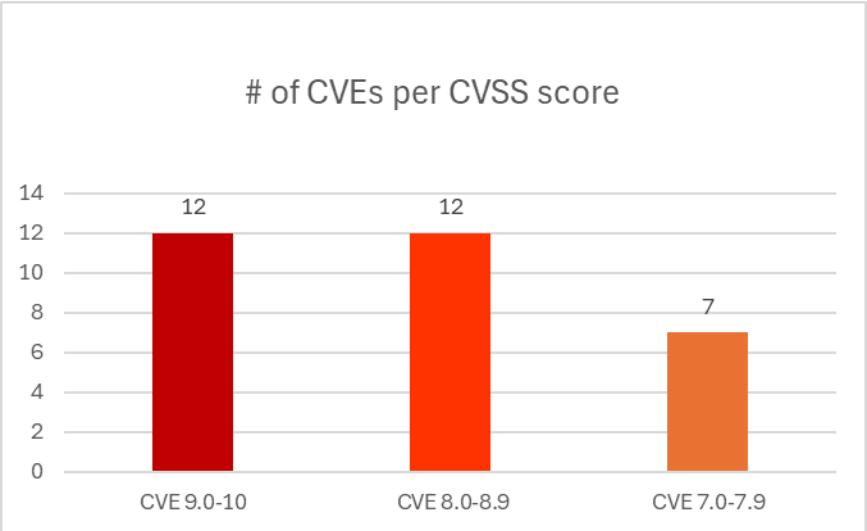
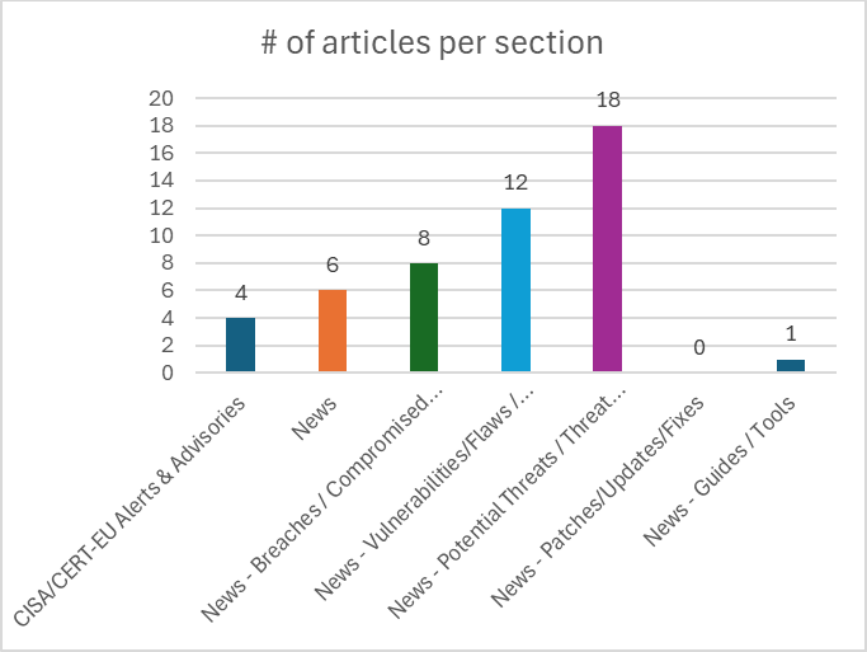
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 03/06/2026 - 05/06/2026





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-2026-48567	**10**	Azure HorizonDB	Authentication Bypass by Spoofing	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48567
https://nvd.nist.gov/vuln/detail/CVE-2019-25729	**9,8**	PDF Signer	Cross-Site Request Forgery (CSRF)	PDF Signer 3.0	https://codecanyon.net/item/signer-create-digital-signatures-and-sign-pdf-documents-online/20737707 https://codecanyon.net/user/simcy_creative https://www.exploit-db.com/exploits/46276 https://www.vulncheck.com/advisories/pdf-signer-server-side-template-injection-rce-via-csrf-cookie
https://nvd.nist.gov/vuln/detail/CVE-2019-25741	**9,8**	Mobatek	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Mobatek MobaXterm 12.1	https://download.mobatek.net/1112019010310554/MobaXterm_Portable_v11.1.zip https://www.exploit-db.com/exploits/47429 https://www.vulncheck.com/advisories/mobatek-mobaxterm-buffer-overflow-via-sessions-file
https://nvd.nist.gov/vuln/detail/CVE-2025-67447	**9,8**	Neterbit	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Neterbit NW-431F Router 20241014-IR03 and before	https://github.com/fun-beep/CVEs/tree/main/CVE-2025-67447 https://neterbit.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-71316	**9,8**	SQLite	Improper Handling of Unicode Encoding	Fixed on or around 2025-12-26	https://i.blackhat.com/EU-24/Presentations/EU-24-Tsai-V2-WorstFit-Unveiling-Hidden-Transformers-in-Windows-ANSI.pdf https://learn.microsoft.com/en-us/windows/win32/api/processenv/nf-processenv-getcommandlinea#security-remarks https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2026/va-26-155-01.json https://sqlite.org/src/file/tool/winmain.c https://www.cve.org/CVERecord?id=CVE-2025-71316
https://nvd.nist.gov/vuln/detail/CVE-2026-10880	**9,8**	OSNexus QuantaStor SDS Manager	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	-	https://blog.blacklanternsecurity.com/p/cve-2026-10880-osnexus-quantastor
https://www.cve.org/CVERecord?id=CVE-2026-45247	**9,8**	Mirasvit	Deserialization of Untrusted Data	Mirasvit Full Page Cache Warmer for Magento 2 before version 1.11.12	https://sansec.io/research/mirasvit-cache-warmer-object-injection https://mirasvit.com/package/changelog/?package=mirasvit/module-cache-warmer https://www.vulncheck.com/advisories/mirasvit-cache-warmer-for-magento-php-object-injection

https://nvd.nist.gov/vuln/detail/CVE-2026-10840	9,6	OpenShift Pipelines	Incorrect Permission Assignment for Critical Resource	-	https://access.redhat.com/security/cve/CVE-2026-10840 https://bugzilla.redhat.com/show_bug.cgi?id=2484720
https://nvd.nist.gov/vuln/detail/CVE-2026-10881	9,6	Google Chrome	Out-of-bounds Read, Out-of-bounds Write	Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/498904293
https://nvd.nist.gov/vuln/detail/CVE-2026-10886	9,6	Google Chrome	Use After Free	Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/505096898
https://nvd.nist.gov/vuln/detail/CVE-2026-48579	9,1	Microsoft Exchange Online	Improper Authorization	Microsoft Exchange Online	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48579
https://nvd.nist.gov/vuln/detail/CVE-2026-50076	9,1	Apache Fory	Deserialization of Untrusted Data	Java SDK before 1.1.0	http://www.openwall.com/lists/oss-security/2026/06/04/4 https://fory.apache.org/security
https://nvd.nist.gov/vuln/detail/CVE-2026-43984	8,9	Tautulli	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Versions prior to 2.17.1	https://github.com/Tautulli/Tautulli/releases/tag/v2.17.1 https://github.com/Tautulli/Tautulli/security/advisories/GHSA-f4j7-pjwc-4jrr
https://nvd.nist.gov/vuln/detail/CVE-2026-10891	8,8	GFX in Google Chrome on Linux	Use After Free	GFX in Google Chrome on Linux prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/513160681
https://nvd.nist.gov/vuln/detail/CVE-2026-11076	8,8	CSS in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	CSS in Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/499784386
https://nvd.nist.gov/vuln/detail/CVE-2026-11147	8,8	WebML in Google Chrome on Window	Use After Free	WebML in Google Chrome on Windows prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/501731689
https://nvd.nist.gov/vuln/detail/CVE-2026-11171	8,8	Blink in Google Chrome	External Control of Assumed-Immutable Web Parameter	Blink in Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/502322843
https://nvd.nist.gov/vuln/detail/CVE-2026-11173	8,8	V8 in Google Chrome	Out-of-bounds Write	V8 in Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/502337304
https://nvd.nist.gov/vuln/detail/CVE-2026-11262	8,8	TabStrip in Google Chrome	Use After Free	TabStrip in Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/499386363
https://nvd.nist.gov/vuln/detail/CVE-2026-11279	8,8	DevTools in Google Chrome	Out-of-bounds Read	in DevTools in Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/501878477
https://nvd.nist.gov/vuln/detail/CVE-2026-11307	8,8	PDFium	Use After Free	PDFium in Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/504551617
https://nvd.nist.gov/vuln/detail/CVE-2025-69755	8,2	Neterbit NW-431F Router	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Neterbit NW-431F Router vNW-431F-20241014-IR03	https://github.com/fun-beep/CVEs/tree/main/CVE-2025-69755 https://neterbit.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-48681	8,1	OpenStack Ironic	Relative Path Traversal	OpenStack Ironic through before 35.0.2	http://www.openwall.com/lists/oss-security/2026/06/03/12 https://bugs.launchpad.net/ironic/+bug/2148333

					https://www.openwall.com/lists/oss-security/2026/06/03/12
https://nvd.nist.gov/vuln/detail/CVE-2026-11241	**8,0**	Cast in Google Chrome	Improper Input Validation	Cast in Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/497203741
https://nvd.nist.gov/vuln/detail/CVE-2026-20245	**7,8**	Cisco Catalyst SD-WAN Manager	Improper Encoding or Escaping of Output	CLI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
https://nvd.nist.gov/vuln/detail/CVE-2026-41234	**7,6**	Froxlor	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Prior to version 2.3.7	https://github.com/advisories/GHSA-x6w6-2xwp-3jh6 https://github.com/froxlor/froxlor/releases/tag/2.3.7 https://github.com/froxlor/froxlor/security/advisories/GHSA-37m5-m4q3-fc6x
https://nvd.nist.gov/vuln/detail/CVE-2026-11058	**7,5**	CredentialProvider in Google Chrome on Windows	External Control of Assumed-Immutable Web Parameter	CredentialProvider in Google Chrome on Windows prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/498986406
https://nvd.nist.gov/vuln/detail/CVE-2026-11296	**7,5**	ImageCapture in Google Chrome	Improper Privilege Management	ImageCapture in Google Chrome prior to 149.0.7827.53	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/502493950
https://nvd.nist.gov/vuln/detail/CVE-2026-8888	**7,5**	Securly Chrome Extension	Inefficient Regular Expression Complexity	Version 3.0.7	https://kb.cert.org/vuls/id/595768
https://nvd.nist.gov/vuln/detail/CVE-2026-36611	**7,3**	Mercusys	Exposure of Sensitive Information to an Unauthorized Actor	Mercusys AC12G (EU) V1 with firmware AC12G(EU)_V1_200909	https://github.com/Tymbark7372/MERCUSYS-AC12G/blob/master/advisories/CVE-2026-36611.md
https://nvd.nist.gov/vuln/detail/CVE-2026-3820	**7,2**	Supermicro	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Supermicro BMC SMTP service at Supermicro AS-2115HS-TNR	https://www.supermicro.com/en/support/security_BMC_IPMI_Jun_2026

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 and Partners Urge Hardening Automatic Tank Gauge Systems		https://www.cisa.gov/resources-tools/resources/cisa-and-partners-urge-hardening-automatic-tank-gauge-systems
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2022-0492 Linux Kernel Improper Authentication Vulnerability ▪ CVE-2025-48595 Android Framework Integer Overflow Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/02/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-45247 Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/03/cisa-adds-one-known-exploited-vulnerability-catalog
Critical Vulnerability in PAN-OS		https://cow-prod-www-v3.azurewebsites.net/publications/security-advisories/2026-006/

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
Let’s Encrypt Unveils Merkle Tree Certificates to Secure the Web Against Quantum Threats	https://cybersecuritynews.com/lets-encrypt-merkle-tree-certificates/
Dashlane Details How Hackers Managed to Download Encrypted Password Vaults	https://cybersecuritynews.com/dashlane-encrypted-password-hack/
Cybercriminals Shift From Fake Login Pages to Infostealer Malware in Phishing Attacks	https://cybersecuritynews.com/cybercriminals-shift-from-fake-login-pages/
Bots Surpass Humans in Global Web Traffic for the First Time in Internet History	https://cybersecuritynews.com/bots-surpass-humans-in-web-traffic/
Microsoft Unveils Always-On AI Agent Scout to Integrate With Teams, Outlook, and More	https://cybersecuritynews.com/microsoft-unveils-scout-ai-agent/
Microsoft 365 Android Apps Account Takeover Vulnerability Impacted Billions of Android Users	https://cybersecuritynews.com/microsoft-365-android-apps-account-takeover-vulnerability/

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
binding.gyp Supply Chain Attack Compromises Dozens of npm Packages Across Maintainer Accounts	https://cybersecuritynews.com/binding-gyp-supply-chain-attack-compromises-dozens-of-npm-packages/
Stock Exchange Executive's Outlook Account Targeted to Exfiltrate Credentials	https://cybersecuritynews.com/stock-exchange-executives-outlook-account-targeted/
CISA Warns of critical Magento Cache Warmer RCE flaw Exploited in Attacks	https://cybersecuritynews.com/magento-cache-warmer-rce-flaw-exploited/
Anthropic's Claude Oceanus-v1-p Opens to Red Team Testing, but Distribution is Compromised	https://cybersecuritynews.com/anthropics-claude-oceanus-v1-p/
Hackers Actively Exploiting WordPress Plugin Vulnerability to Inject Malicious PHP Code	https://cybersecuritynews.com/wordpress-plugin-vulnerability-exploit/
Teams and Google Drive Leveraged to Compromise Systems Within 20 Minutes	https://cybersecuritynews.com/microsoft-teams-and-google-drive-abused/
New Google Gemini Vulnerability Exploited via Prompt Injections from WhatsApp, Slack, and SMS	https://cybersecuritynews.com/google-gemini-vulnerability-exploited/
WordPress Plugin Vulnerability Exposes 500,000+ Websites to Privilege Escalation Attacks	https://cybersecuritynews.com/wordpress-plugin-vulnerability-exposes-2/

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
Cisco SD-WAN Vulnerability Exploited in the Wild to Execute Arbitrary Commands as Root User	https://cybersecuritynews.com/cisco-sd-wan-vulnerability-exploit/
Microsoft Edge Vulnerability Allows Remote Attackers to Execute Arbitrary Code	https://cybersecuritynews.com/microsoft-edge-vulnerability-code-execution/
Comodo Internet Security 0-Day Vulnerability Lets Attacker Crash the User's Windows System	https://cybersecuritynews.com/comodo-internet-security-0-day-vulnerability/
Cisco Unified Communications Manager Vulnerability Exposed Along With PoC Exploit Code	https://cybersecuritynews.com/cisco-unified-communications-manager-vulnerability/
CISA Warns of Android Framework Integer Overflow Vulnerability Exploited in Attacks	https://cybersecuritynews.com/android-framework-integer-overflow-vulnerability-exploited/
Acer Working to Patch Wave 7 Router 0-day Vulnerability	https://cybersecuritynews.com/acer-patch-wave-7-router-0-day-vulnerability/
Five OpenClaw 0-Days let Attackers to Hijack Trusted AI Agent Access	https://cybersecuritynews.com/five-openclaw-0-days/
Critical Apache ActiveMQ Vulnerability Allows Malicious Security Header Injections	https://cybersecuritynews.com/apache-activemq-header-injection-vulnerability/
Ivanti ITSM Vulnerability Lets Attackers Gain Admin Privilege	https://cybersecuritynews.com/ivanti-itsm-vulnerability-admin-privilege/
Laravel CRLF Injection Vulnerability Enables an Attacker to Interfere with Outbound Email Processing	https://cybersecuritynews.com/laravel-crlf-injection-vulnerability/
Windows Search URI Handler Flaw Leaks NTLMv2 Hashes to Attacker-Controlled Servers	https://cybersecuritynews.com/windows-search-uri-flaw-leaks-ntlmv2-hashes/
1-Click GitHub Token Vulnerability Lets Attackers Steal Users' OAuth Tokens	https://cybersecuritynews.com/1-click-github-token-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

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
VECT 2.0 Ransomware Can Damage Files Its Own Decryptor Cannot Reliably Restore	https://cybersecuritynews.com/vect-2-0-ransomware-can-damage-files-its-own-decryptor/
ClawHub, Cisco, Vercel's Malicious Skill Detector Bypassed to upload Malicious Skills	https://cybersecuritynews.com/clawhub-cisco-vercels-malicious-skill-detector-bypassed/
Hackers Impersonate Ghidra, dnSpy, and SpiderFoot to Spread Malware via Fake Download Sites	https://cybersecuritynews.com/hackers-impersonate-ghidra-dnspy-and-spiderfoot/
Hackers Use Malicious Ads to Deliver FlutterShell Backdoor on macOS Systems	https://cybersecuritynews.com/hackers-use-malicious-ads/
Hackers Use Fake Claude Code Install Page to Deliver Fileless .NET Infostealer	https://cybersecuritynews.com/hackers-use-fake-claude-code-install-page/
IronWorm Supply Chain Attack Uses Malicious npm Packages to Steal Developer Se-crets	https://cybersecuritynews.com/ironworm-supply-chain-attack-uses-malicious-npm-packages/
Proofpoint Warns TA4922 Deploys Atlas RAT, RomulusLoader, SilentRunLoader, and ValleyRAT	https://cybersecuritynews.com/proofpoint-warns-ta4922-deploys-atlas-rat/
Weaponized ChatGPT Download Site Delivers Malware Via Sponsored Search Re-sults	https://cybersecuritynews.com/weaponized-chatgpt-download-site-delivers-malware/
Kali365 PhaaS Operation Expands Beyond Microsoft 365 to Target Okta and MAX Messenger	https://cybersecuritynews.com/kali365-phaas-operation-expands-beyond-microsoft-365/
Payouts King Ransomware Evades EDR With Obfuscation and Direct System Calls	https://cybersecuritynews.com/payouts-king-ransomware-evades-edr/
Hackers Use Fake Chrome Web Store Copyright Notices to Steal Google Credentials	https://cybersecuritynews.com/hackers-use-fake-chrome-web-store-copyright-notices/
Fake Claude Code Installer Via Google Sites Delivers Credential-Stealing Malware	https://cybersecuritynews.com/fake-claude-code-installer-via-google-sites/
HazyBeacon Camapign Weaponizes Amazon Web Services for Stealthy Communica-tions	https://cybersecuritynews.com/hazybeacon-camapign-weaponizes-amazon-web-services/
The Gentlemen Ransomware Group Uses Fortinet Exploits, AI, and Custom C2 Frameworks	https://cybersecuritynews.com/the-gentlemen-ransomware-group-uses-fortinet-exploits/
Hackers Use Fake Purchase Orders to Deploy JS.MonoGlyphRAT Targeting US Enter-prises	https://cybersecuritynews.com/hackers-use-fake-purchase-orders-to-deploy-js-monoglyphrat/
Hackers Using AI Tools to Automate Active Directory Attacks and EDR Evasion	https://cybersecuritynews.com/hackers-using-ai-red-team-tools/
Hackers Use YouTube and SEO Poisoning to Spread WeedHack Minecraft Malware	https://cybersecuritynews.com/hackers-use-youtube-and-seo-poisoning/
HTTP/2 Bomb — Remote DoS Exploit Hits nginx, Apache, IIS, Envoy, and Cloudflare Pingora	https://cybersecuritynews.com/http-2-bomb-remote-dos-exploit/

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
HexStrike AI RED-TEAM With 127 Security Tools and BOAZ Red Team Integration	https://cybersecuritynews.com/hexstrike-ai-red-team-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/