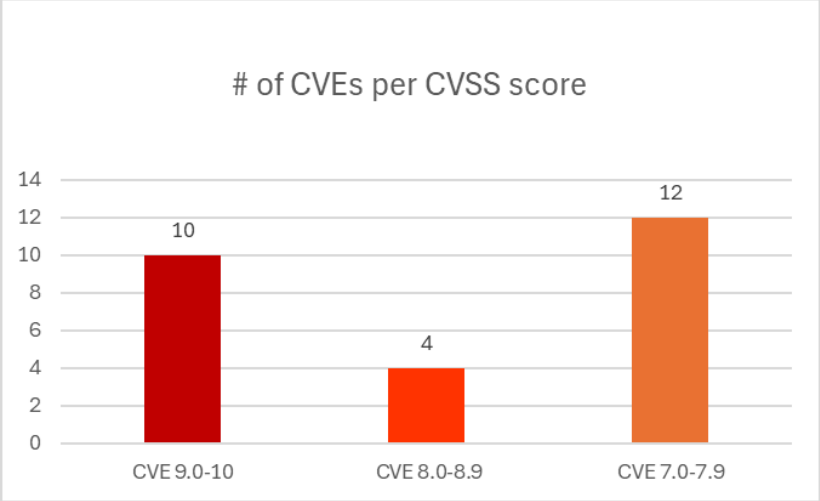
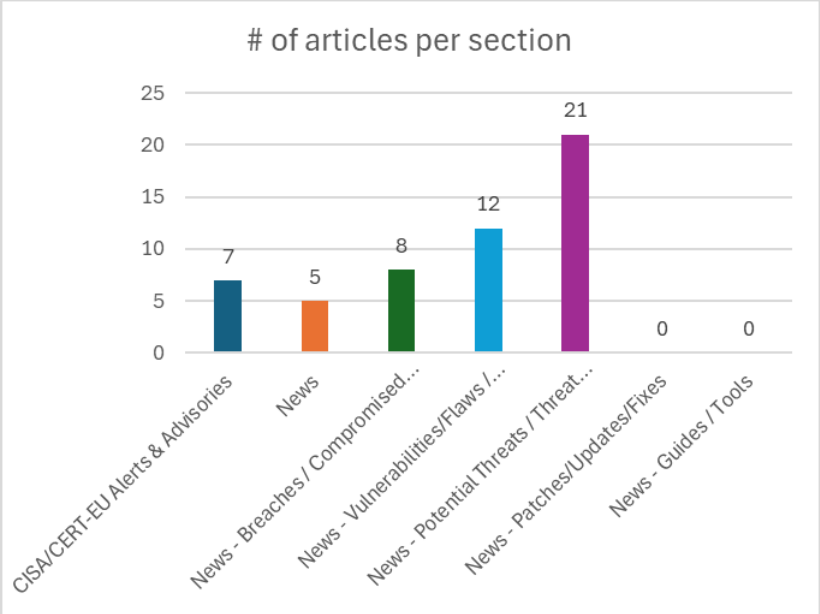
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 22/04/2026 - 24/04/2026





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)	CVSS v3	Προϊόν/ Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-33819	10,0	Microsoft Bing	Deserialization of Untrusted Data	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33819
https://nvd.nist.gov/vuln/detail/CVE-2026-35431	10,0	Microsoft Entra ID Entitlement Management	Server-Side Request Forgery (SSRF)	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35431
https://nvd.nist.gov/vuln/detail/CVE-2026-31181	9,8	ToToLink	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	ToToLink A3300R firmware v17.0.0cu.557_B20221024	https://github.com/Svigo-o/TOTOLINK-Vul/tree/main/totolink-a3300r-stun-server-addr-cmd-injection
https://nvd.nist.gov/vuln/detail/CVE-2026-6748	9,8	Mozilla Corporation	Use of Uninitialized Variable	Uninitialized memory in the Audio/Video: Web Codecs component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	https://bugzilla.mozilla.org/show_bug.cgi?id=2022604 https://www.mozilla.org/security/advisories/mfsa2026-30/ https://www.mozilla.org/security/advisories/mfsa2026-32/ https://www.mozilla.org/security/advisories/mfsa2026-33/ https://www.mozilla.org/security/advisories/mfsa2026-34/
https://nvd.nist.gov/vuln/detail/CVE-2026-6750	9,8	Mozilla Corporation	Improper Privilege Management	Privilege escalation in the Graphics: WebRender component. This vulnerability was fixed in Firefox 150, Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	https://bugzilla.mozilla.org/show_bug.cgi?id=2023407 https://www.mozilla.org/security/advisories/mfsa2026-30/ https://www.mozilla.org/security/advisories/mfsa2026-31/ https://www.mozilla.org/security/advisories/mfsa2026-32/ https://www.mozilla.org/security/advisories/mfsa2026-33/ https://www.mozilla.org/security/advisories/mfsa2026-34/
https://nvd.nist.gov/vuln/detail/CVE-2026-6760	9,8	Mozilla Corporation	Authentication Bypass Using an Alternate Path or Channel	Mitigation bypass in the Networking: Cookies component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	https://bugzilla.mozilla.org/show_bug.cgi?id=2016923 https://www.mozilla.org/security/advisories/mfsa2026-30/ https://www.mozilla.org/security/advisories/mfsa2026-33/

https://nvd.nist.gov/vuln/detail/CVE-2026-6768	9,8	Mozilla Corporation	Authentication Bypass Using an Alternate Path or Channel	Mitigation bypass in the Networking: Cookies component. This vulnerability was fixed in Firefox 150 and Thunderbird 150.	https://bugzilla.mozilla.org/show_bug.cgi?id=2023615 https://www.mozilla.org/security/advisories/mfsa2026-30/ https://www.mozilla.org/security/advisories/mfsa2026-33/
https://nvd.nist.gov/vuln/detail/CVE-2026-6771	9,8	Mozilla Corporation	Authentication Bypass Using an Alternate Path or Channel	Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 150, Firefox ESR 140.10, Thunderbird 150, and Thunderbird 140.10.	https://bugzilla.mozilla.org/show_bug.cgi?id=2025067 https://www.mozilla.org/security/advisories/mfsa2026-30/ https://www.mozilla.org/security/advisories/mfsa2026-32/ https://www.mozilla.org/security/advisories/mfsa2026-33/ https://www.mozilla.org/security/advisories/mfsa2026-34/
https://nvd.nist.gov/vuln/detail/CVE-2026-6887	9,8	BorG Technology Corporation	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Borg SPM 2007 (Sales Ended in 2008) developed by BorG Technology Corporation	https://www.twcert.org.tw/en/cp-139-10863-2f48e-2.html https://www.twcert.org.tw/tw/cp-132-10861-b8709-1.html
https://www.cve.org/CVERecord?id=CVE-2026-39987	9,3	Marimo	Missing Authentication for Critical Function	marimo is a reactive Python notebook. Prior to 0.23.0	github.com: https://github.com/marimo-team/marimo/security/advisories/GHSA-2679-6mx9-h9xc github.com: https://github.com/marimo-team/marimo/pull/9098 github.com: https://github.com/marimo-team/marimo/commit/c24d4806398f30be6b12acd6c60d1d7c68cfd12a
https://nvd.nist.gov/vuln/detail/CVE-2026-26150	8,6	Microsoft Purview	Server-Side Request Forgery (SSRF)	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26150
https://www.cve.org/CVERecord?id=CVE-2023-27351	8,2	PaperCut	Improper Authentication	PaperCut NG 22.0.5 (Build 63914)	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219 https://www.zerodayinitiative.com/advisories/ZDI-23-232/
https://nvd.nist.gov/vuln/detail/CVE-2026-26354	8,1	Dell	Stack-based Buffer Overflow	Dell PowerProtect Data Domain with Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.60	https://www.dell.com/support/kbdoc/en-us/000450699/dsa-2026-060-security-update-for-dell-power-protect-data-domain-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2026-32172	8,0	Microsoft Power Apps	Uncontrolled Search Path Element	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32172

https://www.cve.org/CVERecord?id=CVE-2026-33825	7,8	Microsoft Defender	Insufficient Granularity of Access Control	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825
https://nvd.nist.gov/vuln/detail/CVE-2026-35245	7,5	Oracle VM VirtualBox	Improper Access Control	The supported version that is affected is 7.2.6. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5	https://www.oracle.com/security-alerts/cpuapr2026.html
https://nvd.nist.gov/vuln/detail/CVE-2026-3621	7,5	IBM WebSphere Application Server	Improper Privilege Management	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.4 IBM WebSphere Application Server Liberty	https://www.ibm.com/support/pages/node/7270437
https://nvd.nist.gov/vuln/detail/CVE-2026-6784	7,5	Mozilla Corporation	Out-of-bounds Read	Firefox 149 and Thunderbird 149	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1536243%2C1745382%2C1851073%2C1893400%2C1963301%2C2001319%2C2002899%2C2012436%2C2014435%2C2016901%2C2019916%2C2020486%2C2020612%2C2020817%2C2021788%2C2022051%2C2022367%2C2022431%2C2023302%2C2023670%2C2024225%2C2024238%2C2024240%2C2024265%2C2024367%2C2024369%2C2024424%2C2024760%2C2025281%2C2025361%2C2025387%2C2025466%2C2025954%2C2025958%2C2026278%2C2026292%2C2026297%2C2026378%2C2027148%2C2027287%2C2027341%2C2027384%2C2027427%2C2027694%2C2027993%2C2028009%2C2028270%2C2028416%2C2028524%2C2029295%2C2029301%2C2029461%2C2029699%2C2029800%2C2029801 https://www.mozilla.org/security/advisories/mfsa2026-30/ https://www.mozilla.org/security/advisories/mfsa2026-33/
https://nvd.nist.gov/vuln/detail/CVE-2026-6903	7,5	LabOne Web Server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	-	https://www.zhinst.com/support/download-center/ https://www.zhinst.com/support/security/2026/zi-sa-2026-001/
https://nvd.nist.gov/vuln/detail/CVE-2026-6947	7,5	D-Link	Improper Restriction of Excessive Authentication Attempts	DWM-222W USB Wi-Fi Adapter developed by D-Link	https://www.twcert.org.tw/en/cp-139-10865-de323-2.html https://www.twcert.org.tw/tw/cp-132-10864-944b1-1.html
https://www.cve.org/CVE-Record?id=CVE-2026-20128	7,5	Cisco Catalyst	Storing Passwords in a Recoverable Format	Data Collection Agent (DCA) feature of Cisco Catalyst SD-WAN Manager could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

https://nvd.nist.gov/vuln/detail/CVE-2026-41355	7,3	OpenShell	Inclusion of Functionality from Untrusted Control Sphere	OpenShell before 2026.3.28	https://github.com/openclaw/openclaw/commit/c02ee8a3a4cb390b23afdf21317aa8b2096854d1 https://github.com/openclaw/openclaw/security/advisories/GHSA-42mx-vp8m-j7qh https://www.vulncheck.com/advisories/openshell-arbitrary-code-execution-via-mirror-mode-sandbox-file-conversion
https://www.cve.org/CVERecord?id=CVE-2024-27199	7,3	JetBrains TeamCity	-	JetBrains TeamCity before 2023.11.4	https://www.jetbrains.com/privacy-security/issues-fixed/ https://www.darkreading.com/cyberattacks-data-breaches/jetbrains-teamcity-mass-exploitation-underway-rogue-accounts-thrive
https://nvd.nist.gov/vuln/detail/CVE-2026-34292	7,2	Oracle WebLogic Server	Improper Access Control	Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts).	https://www.oracle.com/security-alerts/cpuapr2026.html
https://www.cve.org/CVERecord?id=CVE-2025-2749	7,2	Kentico Xperience	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	This issue affects Kentico Xperience through 13.0.178	https://labs.watchtowr.com/bypassing-authentication-like-its-the-90s-pre-auth-rce-chain-s-in-kentico-xperience-cms/ https://devnet.kentico.com/download/hotfixes https://www.vulncheck.com/advisories/kentico-xperience-staging-media-file-upload-authenticated-rce
https://nvd.nist.gov/vuln/detail/CVE-2026-41361	7,1	OpenClaw	Incomplete List of Disallowed Inputs	OpenClaw before 2026.3.28	https://github.com/openclaw/openclaw/security/advisories/GHSA-g86v-f9qv-rh6m https://www.vulncheck.com/advisories/openclaw-ssrf-guard-bypass-via-ipv6-special-use-ranges

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
Supply Chain Compromise Impacts Axios Node Package Manager		https://www.cisa.gov/news-events/alerts/2026/04/20/supply-chain-compromise-impacts-axios-node-package-manager
CISA Adds Eight Known Exploited Vulnerabilities to Catalog	▪ CVE-2023-27351 PaperCut NG/MF Improper Authentication Vulnerability ▪ CVE-2024-27199 JetBrains TeamCity Relative Path Traversal Vulnerability ▪ CVE-2025-2749 Kentico Xperience Path Traversal Vulnerability ▪ CVE-2025-32975 Quest KACE Systems Management Appliance (SMA) Improper Authentication Vulnerability ▪ CVE-2025-48700 Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability ▪ CVE-2026-20122 Cisco Catalyst SD-WAN Manager Incorrect Use of Privileged APIs Vulnerability ▪ CVE-2026-20128 Cisco Catalyst SD-WAN Manager Storing Passwords in a Recoverable Format Vulnerability ▪ CVE-2026-20133 Cisco Catalyst SD-WAN Manager Exposure of Sensitive Information to an Unauthorized Actor Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/20/cisa-adds-eight-known-exploited-vulnerabilities-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-33825 Microsoft Defender Insufficient Granularity of Access Control Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/22/cisa-adds-one-known-exploited-vulnerability-catalog
FIRESTARTER Backdoor		https://www.cisa.gov/news-events/analysis-reports/ar26-113a
Defending Against China-Nexus Covert Networks of Compromised Devices		https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-39987 Marimo Remote Code Execution Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/23/cisa-adds-one-known-exploited-vulnerability-catalog
V1: ED 25-03: Identify and Mitigate Potential Compromise of Cisco Devices		https://www.cisa.gov/news-events/directives/v1-ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices

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
Microsoft Teams Issue Blocking Users From Joining Meetings Following Edge browser update	https://cybersecuritynews.com/microsoft-teams-issue-blocking-users/
Microsoft Teams Rolls Out Efficiency Mode to Optimize Performance on Low-End Devices	https://cybersecuritynews.com/microsoft-teams-efficiency-mode/
Massive SIM Farm-as-a-Service Network Exposes 87 Control Panels Across 17 Countries	https://cybersecuritynews.com/sim-farm-as-a-service-network/
Where Most SOCs Stall: Building SOC Maturity with Threat Intelligence Feeds	https://cybersecuritynews.com/soc-maturity-threat-intelligence/
Hackers Use Nightmare-Eclipse Tools After Compromising FortiGate SSL VPN Access	https://cybersecuritynews.com/nightmare-eclipse-tools-fortigate-ssl-vpn/

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 Leverage Microsoft Teams to Breach Organizations Posing as IT Helpdesk Staff	https://cybersecuritynews.com/microsoft-teams-breach-organizations/
Bitwarden CLI Compromised in Supply Chain Attack via GitHub Actions	https://cybersecuritynews.com/bitwarden-cli-compromised/
Vercel Confirms Security Breach – Set of Customer Account Compromised	https://cybersecuritynews.com/vercel-confirms-security-breach/
Checkmarx KICS Official Docker Repo Compromised to Inject Malicious Code	https://cybersecuritynews.com/checkmarx-kics-compromised/
The Phishing Defense Layer Top CISOs Never Miss	https://cybersecuritynews.com/phishing-defense-layer/
12 Browser Extensions Mimic as TikTok Video Downloaders Compromised 130k Users	https://cybersecuritynews.com/browser-extensions-as-tiktok-video-downloaders/
CISA Warns Axios npm Package Was Compromised in Major Supply Chain Attack	https://cybersecuritynews.com/cisa-warns-axios-npm-supply-chain/
Unauthorized Group Gains Access to Anthropic’s Exclusive Cyber Tool Mythos	https://cybersecuritynews.com/anthropic-mythos-access/

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 Pack2TheRoot Vulnerability Let Attackers Gain Root Access or Compromise the System	https://cybersecuritynews.com/pack2theroot-vulnerability/
Apple Fixes Notification Privacy Flaw That Allowed FBI to Access Deleted Signal Messages	https://cybersecuritynews.com/apple-fixes-notification-privacy-flaw/
Critical Atlassian Bamboo Data Center and Server Flaw Enables Command Injection Attacks	https://cybersecuritynews.com/bamboo-data-center-and-server-vulnerability-2/
1,370+ Microsoft SharePoint Servers Vulnerable to Spoofing Attacks Exposed Online	https://cybersecuritynews.com/1370-sharepoint-servers-vulnerable/
CrowdStrike LogScale Vulnerability Allows Remote Attackers to Read Arbitrary Files from Server	https://cybersecuritynews.com/crowdstrike-logscale-vulnerability/
Microsoft Emergency .NET 10.0.7 Update to Patch Elevation of Privilege Vulnerability	https://cybersecuritynews.com/emergency-net-10-0-7-update-patch/
CISA Warns of Cisco Catalyst SD-WAN Manager Vulnerabilities Exploited in Attacks	https://cybersecuritynews.com/cisco-sd-wan-manager-vulnerabilities/
6000+ Apache ActiveMQ Instances Vulnerable to CVE-2026-34197 Exposed Online	https://cybersecuritynews.com/apache-activemq-instances-exposed/
Hackers Could Weaponize GGUF Models to Achieve RCE on SGLang Inference Servers	https://cybersecuritynews.com/hackers-weaponize-gguf-models/
Claude Code, Gemini CLI, and GitHub Copilot Vulnerable to Prompt Injection via GitHub Comments	https://cybersecuritynews.com/prompt-injection-via-github-comments/
Claude Mythos AI Model Uncovers 271 Zero-Day Vulnerabilities in Firefox	https://cybersecuritynews.com/claude-mythos-271-zero-days/
PoC Exploit Released for Windows Snipping Tool NTLM Hash Leak Vulnerability	https://cybersecuritynews.com/windows-snipping-tool-ntlm-hash/

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
Malicious npm Package Turns Hugging Face Into Malware CDN and Exfiltration Backend	https://cybersecuritynews.com/malicious-npm-package-turns-hugging-face/
AI-Assisted Lazarus Campaign Targets Developers With Backdoored Coding Challenges	https://cybersecuritynews.com/ai-assisted-lazarus-campaign-targets/
Hackers Abuse Fake Wallpaper App and YouTube Channel to Spread notnullOSX Malware	https://cybersecuritynews.com/hackers-abuse-fake-wallpaper-app/
Fake TradingView AI Agent Site is Delivering Needle Stealer Malware via Fake TradingClaw	https://cybersecuritynews.com/fake-tradingview-ai-agent-site/
Hackers Use Outlook Mailboxes to Hide Linux GoGra Backdoor Communications	https://cybersecuritynews.com/hackers-use-outlook-mailboxes/
New Tropic Trooper Attack Uses Custom Beacon Listener and VS Code Tunnels for Remote Access	https://cybersecuritynews.com/new-tropic-trooper-attack-uses-custom-beacon-listener/
109 Fake GitHub Repositories Used to Deliver SmartLoader and StealC Malware	https://cybersecuritynews.com/109-fake-github-repositories-used/
Malicious Google Ads Target Crypto Users With Wallet Drainers and Seed Phrase Theft	https://cybersecuritynews.com/malicious-google-ads-target-crypto-users/
Cybercriminals Exploit French Fintech Accounts to Move Stolen Money Before Detection	https://cybersecuritynews.com/cybercriminals-exploit-french-fintech-accounts/
Hackers Use Lotus Wiper to Destroy Drives and Delete Files in Energy Sector Attack	https://cybersecuritynews.com/hackers-use-lotus-wiper-to-destroy-drives/
Microsoft Warns Jasper Sleet Uses Fake IT Worker Identities to Infiltrate Cloud Environments	https://cybersecuritynews.com/microsoft-warns-jasper-sleet-uses-fake-it-worker-identities/
New Auraboros RAT Exposes Live Audio Streaming, Keylogging, and Cookie Hijacking in Open C2 Panel	https://cybersecuritynews.com/new-auraboros-rat-exposes-live-audio-streaming-keylogging/
New DinDoor Backdoor Abuses Deno Runtime and MSI Installers to Evade Detection	https://cybersecuritynews.com/new-dindoor-backdoor-abuses-deno-runtime/
Compromised Namastex npm Packages Deliver TeamPCP-Style CanisterWorm Malware	https://cybersecuritynews.com/compromised-namastex-npm-packages/
Microsoft-Signed Binary Used to Sneak LOTUSLITE Into India-Focused Espionage Campaign	https://cybersecuritynews.com/microsoft-signed-binary-used-to-sneak-lotuslite/
New NGate Malware Developed Using AI Hides in NFC Payment Apps	https://cybersecuritynews.com/new-ngate-malware-developed/
New PureRAT Campaign Hides PE Payloads in PNG Files and Executes Them Filelessly	https://cybersecuritynews.com/new-purerat-campaign-hides-pe-payloads/
Hackers Abuse GitHub Issue Notifications to Phish Developers Through Malicious OAuth Apps	https://cybersecuritynews.com/hackers-abuse-github-issue-notifications/
Gentlemen RaaS Attacking Windows, Linux With additional locker written in C for ESXi	https://cybersecuritynews.com/gentlemen-raas-attacking-windows-linux/
AI-Powered Exploitation May Collapse the Patch Window for Defenders	https://cybersecuritynews.com/ai-powered-exploitation-may-collapse/
SideWinder Uses Fake Chrome PDF Viewer and Zimbra Clone to Steal Government Webmail Credentials	https://cybersecuritynews.com/sidewinder-uses-fake-chrome-pdf-viewer-and-zimbra-clone/

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

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/