Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/04/2026 - 21/04/2026

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)	CVS Sv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-40492	9,8	SAIL	Out-of-bounds Write	Prior to commit 36aa5c7ec8a2bb35f6fb867a1177a6f141156b02	https://github.com/HappySeaFox/sail/commit/36aa5c7ec8a2bb35f6fb867a1177a6f141156b02 GitHub, Inc. https://github.com/HappySeaFox/sail/security/advisories/GHSA-526v-vm72-4v64
https://app.opencve.io/cve/CVE-2026-5963	9,3	EasyFlow .NET developed by Digiwin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://www.twcert.org.tw/en/cp-139-10832-05f3a-2.html https://www.twcert.org.tw/tw/cp-132-10831-a734d-1.html
https://app.opencve.io/cve/CVE-2026-5964	9,3	EasyFlow .NET developed by Digiwi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://www.twcert.org.tw/en/cp-139-10832-05f3a-2.html https://www.twcert.org.tw/tw/cp-132-10831-a734d-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-40258	9,1	The Gramps Web API	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1.6.0 through 3.11.0	https://github.com/gramps-project/gramps-web-api/commit/3ed4342711e3ec849552df09b1fe2fbf2ca5c29a GitHub, Inc. https://github.com/gramps-project/gramps-web-api/releases/tag/v3.11.1 GitHub, Inc. https://github.com/gramps-project/gramps-web-api/security/advisories/GHSA-m5gr-86j6-99jp
https://app.opencve.io/cve/CVE-2026-41329	9,0	OpenClaw	Incorrect Use of Privileged APIs	OpenClaw before 2026.3.31	https://github.com/openclaw/openclaw/commit/a30214a624946fc5c85c9558a27c1580172374fd https://github.com/openclaw/openclaw/security/advisories/GHSA-g5cg-8x5w-7jpm https://www.vulncheck.com/advisories/openclaw-sandbox-bypass-via-heartbeat-context-inheritance-and-senderisowner-escalation
https://nvd.nist.gov/vuln/detail/CVE-2026-40572	9,0	NovumOS	Improper Privilege Management	prior to 0.24	https://github.com/MinecAnton209/NovumOS/releases/tag/v0.24 GitHub, Inc. https://github.com/MinecAnton209/NovumOS/security/advisories/GHSA-rg7m-6vh7-f4v2
https://nvd.nist.gov/vuln/detail/CVE-2026-40487	8,9	Postiz	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to version 2.21.6	https://github.com/gitroomhq/postiz-app/releases/tag/v2.21.6 GitHub, Inc. https://github.com/gitroomhq/postiz-app/security/advisories/GHSA-44wg-r34q-hvfx

https://app.opencve.io/cve/CVE-2026-30898	8,8	Airflow	Improper Neutralization of Special Elements used in a Command ('Command Injection')		http://www.openwall.com/lists/oss-security/2026/04/17/7 https://github.com/apache/airflow/pull/64129 https://lists.apache.org/thread/26zmhfj1t95c1hld2r14ho81nzh1bdc8
https://nvd.nist.gov/vuln/detail/CVE-2026-40350	8,8	Movary	Incorrect Authorization	Prior to version 0.71.1	https://github.com/leepeuker/movary/commit/92c7400486f5fe9f350046e04e45a8502778bf39 GitHub, Inc. https://github.com/leepeuker/movary/pull/749 GitHub, Inc. https://github.com/leepeuker/movary/releases/tag/0.71.1 GitHub, Inc. https://github.com/leepeuker/movary/security/advisories/GHSA-7r3f-9fwv-p43w
https://nvd.nist.gov/vuln/detail/CVE-2026-6518	8,8	The CMP – Coming Soon & Maintenance Plugin by NiteoThemes plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 4.1.16	https://plugins.trac.wordpress.org/browser/cmp-coming-soon-maintenance/tags/4.1.16/niteo-cmp.php#L1421 Wordfence https://plugins.trac.wordpress.org/browser/cmp-coming-soon-maintenance/tags/4.1.16/niteo-cmp.php#L1437 Wordfence https://plugins.trac.wordpress.org/browser/cmp-coming-soon-maintenance/tags/4.1.16/niteo-cmp.php#L1447 Wordfence https://plugins.trac.wordpress.org/changeset?old_path=%2Fcmp-coming-soon-maintenance/tags/4.1.16&new_path=%2Fcmp-coming-soon-maintenance/tags/4.1.17 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/d6fb275b-dbba-46df-b170-977ef4a84c4c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-6630	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda F451 1.0.0.7_cn_svn7958	https://github.com/Jimi-Lab/cve/issues/23 https://vuldb.com/submit/792882 https://vuldb.com/vuln/358264 https://vuldb.com/vuln/358264/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-6632	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda F451 1.0.0.7_cn_svn7958	https://github.com/Jimi-Lab/cve/issues/26 https://vuldb.com/submit/792905 https://vuldb.com/vuln/358266 https://vuldb.com/vuln/358266/cti https://www.tenda.com.cn/
https://app.opencve.io/cve/CVE-2026-5967	8,7	ThreatSonar Anti-Ransomware developed by TeamT5	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://www.twcert.org.tw/en/cp-139-10855-e6d1b-2.html https://www.twcert.org.tw/tw/cp-132-10854-03015-1.html

https://nvd.nist.gov/vuln/detail/CVE-2026-35465	7,5	SecureDrop Client	External Control of File Name or Path	0.17.4 and below	https://github.com/freedomofpress/securedrop-client/blob/8dc8bb6e307b13876d67f72d8a071202e2f39ab5/changelog.md?plain=1#L8 GitHub, Inc. https://github.com/freedomofpress/securedrop-client/commit/e518adaf897e7838467ccf9e1f28152ae6fe3655 GitHub, Inc. https://github.com/freedomofpress/securedrop-client/security/advisories/GHSA-2jrc-x8fq-prvc
https://nvd.nist.gov/vuln/detail/CVE-2026-6577	7,3	liangliangyy DjangoBlog	Improper Authentication	liangliangyy DjangoBlog up to 2.1.0.0	https://github.com/3em0/cve_repo/blob/main/DjangoBlog/Vuln-2-Unauthenticated-GPS-Data-Injection.md https://vuldb.com/submit/790282 https://vuldb.com/vuln/358212 https://vuldb.com/vuln/358212/cti
https://app.opencve.io/cve/CVE-2026-24505	7,2	Dell PowerProtect Data Domain	Improper Input Validation	Dell PowerProtect Data Domain, versions 8.5 through 8.6	https://www.dell.com/support/kbdoc/en-us/000450699/dsa-2026-060-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities
https://app.opencve.io/cve/CVE-2026-26943	7,2	Dell PowerProtect Data Domain	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, 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-powerprotect-data-domain-multiple-vulnerabilities
https://app.opencve.io/cve/CVE-2026-5966	7,2	ThreatSonar Anti-Ransomware developed by TeamT5	Relative Path Traversal		https://www.twcert.org.tw/en/cp-139-10832-05f3a-2.html https://www.twcert.org.tw/tw/cp-132-10831-a734d-1.html

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

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
NSA Reportedly Using Anthropic's Mythos Despite Pentagon Blacklist	https://cybersecuritynews.com/nsa-confirms-anthropics-mythos-use/
NIST Shifts to Risk-Based NVD Model as CVE Submissions Surge 263% Since 2020	https://cybersecuritynews.com/nvd-model-cve-submissions/
OpenAI Expands Cyber Defense Program With GPT-5.4-Cyber Access for Trusted Organizations	https://cybersecuritynews.com/gpt-5-4-cyber-defense-program/
NIST to stop rating non-priority flaws due to volume increase	https://www.bleepingcomputer.com/news/security/nist-to-stop-rating-non-priority-flaws-due-to-volume-increase/
Hackers Fail to Exploit Flaw in Discontinued TP-Link Routers	https://www.securityweek.com/hackers-fail-to-exploit-flaw-in-discontinued-tp-link-routers/

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
British National Admits Hacking Companies and Stealing Millions in Virtual Currency	https://cybersecuritynews.com/british-national-stealing-millions-in-virtual-currency/
Vercel Confirms Data Breach — Hackers Claim Access to Internal Systems	https://cybersecuritynews.com/vercel-data-breach/
Nearly 6 Million Internet-Facing FTP Servers Still Exposed in 2026, Censys Warns	https://cybersecuritynews.com/ftp-servers-exposed/
Fiverr Allegedly Leaks User Information to Google Indexing, Researchers Say	https://cybersecuritynews.com/fiverr-allegedly-leaks-user-information-to-google/
WhatsApp Leaks User Metadata to Attackers	https://www.darkreading.com/endpoint-security/whatsapp-leaks-user-metadata

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
PoC Exploit Released for Windows Snipping Tool NTLM Hash Leak Vulnerability	https://cybersecuritynews.com/windows-snipping-tool-ntlm-hash/
iTerm2 Flaw Abuses SSH Integration Escape Sequences to Turn Text Into Code Execution	https://cybersecuritynews.com/iterm2-flaw-abuses-ssh-integration/
Critical Gardyn Smart Gardens Vulnerabilities Let Attackers Control Devices Remotely	https://cybersecuritynews.com/gardyn-smart-gardens-vulnerabilities/
Critical Anthropic's MCP Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/anthropics-mcp-vulnerability/
Lovable AI App Builder Reportedly Exposes Thousands of Projects Data via API Flaw	https://cybersecuritynews.com/lovable-ai-app-builder-customer-data/
Microsoft Teams Desktop Client Faces Launch Failures After Update Triggers Caching Regression	https://cybersecuritynews.com/microsoft-teams-desktop-client/
Hackers Use CVE-2024-3721 to Infect TBK DVRs With Nexcorium DDoS Malware	https://cybersecuritynews.com/hackers-use-cve-2024-3721-to-infect-tbk-dvrs/
Critical Vulnerability In Flowise Allows Remote Command Execution Via MCP Adapters	https://cybersecuritynews.com/flowise-vulnerability/
PoC Exploit Released for FortiSandbox Vulnerability that Allows Attacker to Execute Commands	https://cybersecuritynews.com/poc-exploit-fortisandbox-vulnerability/
Anthropic MCP Design Vulnerability Enables RCE, Threatening AI Supply Chain	https://thehackernews.com/2026/04/anthropic-mcp-design-vulnerability.html
Attackers Exploit DVR Command Injection Flaw to Deploy Mirai-Based Botnet	https://www.infosecurity-magazine.com/news/mirai-variant-dvr-flaw-iot-botnet/
Critical flaw in Protobuf library enables JavaScript code execution	https://www.bleepingcomputer.com/news/security/critical-flaw-in-protobuf-library-enables-javascript-code-execution/
Serial-to-IP Converter Flaws Expose OT and Healthcare Systems to Hacking	https://www.securityweek.com/serial-to-ip-converter-flaws-expose-ot-and-healthcare-systems-to-hacking/

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
New Windows 11 Dev Build Improves Secure Boot Monitoring and Storage Controls	https://cybersecuritynews.com/windows-11-dev-secure-boot-controls/
Google Uses Gemini AI to Stop Malicious Ads From Threat Actors – 8.3 billion ads Blocked	https://cybersecuritynews.com/gemini-ai-stop-malicious-ads/

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
Gh0st RAT and CloverPlus Adware Delivered Together in New Dual-Payload Malware Campaign	https://cybersecuritynews.com/gh0st-rat-and-cloverplus-adware-delivered-together/
Hackers Use AppDomain Hijacking to Turn Trusted Intel Utility Into Malware Launcher	https://cybersecuritynews.com/hackers-use-appdomain-hijacking/
North Korea-Linked UNC1069 Uses Fake Zoom and Teams Meetings to Hack Crypto Professionals	https://cybersecuritynews.com/north-korea-linked-unc1069-uses-fake-zoom-and-teams-meetings/
Attackers Abuse Microsoft Teams and Quick Assist in New Helpdesk Impersonation Attack Chain	https://cybersecuritynews.com/attackers-abuse-microsoft-teams-and-quick-assist/
Attackers Turn QEMU Into a Stealth Backdoor for Credential Theft and Ransomware	https://cybersecuritynews.com/attackers-turn-qemu-into-a-stealth-backdoor/
ZionSiphon Malware Targets Water Infrastructure Systems	https://www.infosecurity-magazine.com/news/zionsiphon-malware-water/

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
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/