Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 01/04/2025 - 04/04/2025

Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	Συσκευές/Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-31131	**8,6**	YesWiki is a wiki system written in PHP	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		fixed in 4.5.2	https://github.com/YesWiki/yeswiki/commit/f78c915369a60c74ab8f38561ae93a4aaca9b989 https://github.com/YesWiki/yeswiki/security/advisories/GHSA-w34w-fvp3-68xm
https://nvd.nist.gov/vuln/detail/CVE-2025-31132	**8,1**	Raven is an open-source messaging platform	Improper Input Validation		fixed in 2.1.10	https://github.com/The-Commit-Company/raven/security/advisories/GHSA-wmrr-3mrv-2p57
https://nvd.nist.gov/vuln/detail/CVE-2025-31910	**7,6**	BookingPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through 1.1.28	n/a	https://patchstack.com/database/wordpress/plugin/bookingpress-appointment-booking/vulnerability/wordpress-bookingpress-plugin-1-1-28-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-31137	**7,5**	React Router	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	all Remix 2 and React Router 7 consumers using the Express adapter	patched and released in Remix 2.16.3 and React Router 7.4.1	https://github.com/remix-run/react-router/security/advisories/GHSA-4q56-crqp-v477

https://nvd.nist.gov/vuln/detail/CVE-2025-31908	**7,1**	JSON Structuring Markup	Cross-Site Request Forgery (CSRF)	from n/a through 0.1	n/a	https://patchstack.com/database/wordpress/plugin/json-structuring-markup/vulnerability/wordpress-json-structuring-markup-plugin-0-1-csrf-to-stored-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-31906	**7,1**	WP Profitshare	Cross-Site Request Forgery (CSRF)	from n/a through 1.4.9	n/a	https://patchstack.com/database/wordpress/plugin/wp-profitshare/vulnerability/wordpress-wp-profitshare-plugin-1-4-9-csrf-to-stored-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-31904	**7,1**	Ebook Downloader	Cross-Site Request Forgery (CSRF)	from n/a through 1.0	n/a	https://patchstack.com/database/wordpress/plugin/ebook-downloader/vulnerability/wordpress-ebook-downloader-plugin-1-0-csrf-to-stored-xss-vulnerability?_s_id=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Five Industrial Control Systems Advisories	▪ ICSA-25-093-01 Hitachi Energy RTU500 Series ▪ ICSA-25-093-02 Hitachi Energy TRMTracker ▪ ICSA-25-093-03 ABB ACS880 Drives Containing CODESYS RTS ▪ ICSA-25-093-04 ABB Low Voltage DC Drives and Power Controllers CODESYS RTS ▪ ICSA-25-093-05 B&R APROL	https://www.cisa.gov/news-events/alerts/2025/04/03/cisa-releases-five-industrial-control-systems-advisories
NSA, CISA, FBI, and International Partners Release Cybersecurity Advisory on “Fast Flux,” a National Security Threat		https://www.cisa.gov/news-events/alerts/2025/04/03/nsa-cisa-fbi-and-international-partners-release-cybersecurity-advisory-fast-flux-national-security

News

Σύντομη περιγραφή / Τίτλος	URL
CERT-UA Reports Cyberattacks Targeting Ukrainian State Systems with WRECKSTEEL Malware	https://thehackernews.com/2025/04/cert-ua-reports-cyberattacks-targeting.html
Ukraine Blames Russia for Railway Hack, Labels It "Act of Terrorism"	https://www.infosecurity-magazine.com/news/ukraine-russia-railway-hack/
Nearly 600 Phishing Domains Emerge Following Bybit Heist	https://www.infosecurity-magazine.com/news/over-500-phishing-domains-bybit/
China-Linked Threat Group Exploits Ivanti Bug	https://www.darkreading.com/vulnerabilities-threats/china-linked-threat-group-exploits-ivanti-bug
CrushFTP Vulnerability Exploited Following Disclosure Issues	https://www.infosecurity-magazine.com/news/crushftp-flaw-exploited-disclosure/
New Malware Loaders Use Call Stack Spoofing, GitHub C2, and .NET Reactor for Stealth	https://thehackernews.com/2025/04/new-malware-loaders-use-call-stack.html
CISA warns of Fast Flux DNS evasion used by cybercrime gangs	https://www.bleepingcomputer.com/news/security/cisa-warns-of-fast-flux-dns-evasion-used-by-cybercrime-gangs/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Royal Mail Data Breach: No Operational Impact Reported	https://dailysecurityreview.com/security-spotlight/royal-mail-data-breach-no-operational-impact-reported/
Oracle Acknowledges Data Breach and Starts Informing Affected Clients	https://cybersecuritynews.com/oracle-acknowledges-data-breach/
173,000 Patients Affected by Chord Specialty Dental Partners Email Data Breach	https://dailysecurityreview.com/security-spotlight/173000-patients-affected-by-chord-specialty-dental-partners-email-data-breach/
Sensitive Data Breached in Highline Schools Ransomware Incident	https://www.infosecurity-magazine.com/news/sensitive-data-highline-ransomware/
SimonMed Imaging Confirms Cybersecurity Breach in January 2025	https://dailysecurityreview.com/security-spotlight/simonmed-imaging-confirms-cybersecurity-breach-in-january-2025/

Hacker Claims Twilio's SendGrid Data Breach, Selling 848,000 Records	https://hackread.com/hacker-twilio-sendgrid-data-breach-customer-data/
Massive X (Twitter) Data Leak Exposes Over 200 Million User Records	https://securityonline.info/massive-x-twitter-data-leak-exposes-over-200-million-user-records/?&web_view=true
Over 1,500 PostgreSQL Servers Compromised in Fileless Cryptocurrency Mining Campaign	https://thehackernews.com/2025/04/over-1500-postgresql-servers.html

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
CrushFTP CVE-2025-2825 flaw actively exploited in the wild	https://securityaffairs.com/176097/hacking/crushftp-cve-2025-2825-flaw-actively-exploited.html
New Windows 11 trick lets you bypass Microsoft Account requirement	https://www.bleepingcomputer.com/news/microsoft/new-windows-11-trick-lets-you-bypass-microsoft-account-requirement/
Verizon Call Filter API flaw exposed customers' incoming call history	https://www.bleepingcomputer.com/news/security/verizon-call-filter-api-flaw-exposed-customers-incoming-call-history/
U.S. CISA adds Apache Tomcat flaw to its Known Exploited Vulnerabilities catalog	https://securityaffairs.com/176129/security/u-s-cisa-adds-apache-tomcat-flaw-known-exploited-vulnerabilities-catalog.html
Critical Flaw in Apache Parquet Allows Remote Attackers to Execute Arbitrary Code	https://thehackernews.com/2025/04/critical-flaw-in-apache-parquet-allows.html
Urgent Security Alert: Exploited CSLU Backdoor Threatens Cisco Systems	https://dailysecurityreview.com/security-spotlight/urgent-security-alert-exploited-cslu-backdoor-threatens-cisco-systems/
Apple backported fixes for three actively exploited flaws to older devices	https://securityaffairs.com/176119/security/apple-backported-fixes-for-three-actively-exploited-flaws-to-older-devices.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Google Fixed Cloud Run Vulnerability Allowing Unauthorized Image Access via IAM Misuse	https://thehackernews.com/2025/04/google-fixed-cloud-run-vulnerability.html
Chrome 135, Firefox 137 Patch High-Severity Vulnerabilities	https://www.securityweek.com/chrome-135-firefox-137-patch-high-severity-vulnerabilities/
Google Released Second Fix for Quick Share Flaws After Patch Bypass	https://www.securityweek.com/google-released-second-fix-for-quick-share-flaws-after-patch-bypass/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Attackers are targeting CrushFTP vulnerability with public PoC (CVE-2025-2825)	https://www.helpnetsecurity.com/2025/04/01/crushftp-vulnerability-exploitation-cve-2025-2825/
Hunters International Overlaps Hive Ransomware Attacking Windows, Linux, and ESXi Systems	https://cybersecuritynews.com/hunters-international-overlaps-hive-ransomware/
OpenVPN Vulnerability Let Attackers Crash Servers & Execute Remote Code	https://cybersecuritynews.com/openvpn-vulnerability-let-attackers-crash-servers/
North Korean IT worker army expands operations in Europe	https://www.bleepingcomputer.com/news/security/north-korean-it-worker-army-expands-operations-in-europe/
Outlaw Group Uses SSH Brute-Force to Deploy Cryptojacking Malware on Linux Servers	https://thehackernews.com/2025/04/outlaw-group-uses-ssh-brute-force-to.html

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best Cyber Attack Simulation Tools – 2025	https://cybersecuritynews.com/cyber-attack-simulation-tools/
Top Cybersecurity Tools of 2025 To Managing Remote Device Threats	https://cybersecuritynews.com/top-cybersecurity-tools-managing-remote-device-threats/

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.

[3]. Τα CVEs που αφορούν Wordpress plugins θα εμφανίζονται σε ξεχωριστή ενότητα (1.1) σε περιόδους που η εμφάνισή τους είναι ιδιαίτερα αυξημένη.

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/