Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 24/012024 - 28/01/2025

Contents

1 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-2025-22612	10	Coolify (self-hostable tool for managing servers, applications, and databases)	Exposure of Sensitive Information	Prior to version 4.0.0-beta.374	N/A	https://coolify.io/ https://github.com/coollabsio/coolify/security/advisories/GHSA-wg8x-cgq4-vjxj
https://nvd.nist.gov/vuln/detail/CVE-2024-48841	10	FLXEON	PHP Remote File Inclusion	9.3.4 and older	N/A	https://new.abb.com/low-voltage/products/building-automation/product-range/abb-cylon/products-and-downloads/highlights/flxeon-series https://search.abb.com/library/Download.aspx?DocumentID=9AKK108470A5684&LanguageCode=en&DocumentPartId=PDF&Action=Launch
https://nvd.nist.gov/vuln/detail/CVE-2024-56404	9.9	One Identity Identity Manager	Authentication Bypass	9.x before 9.3	N/A	https://www.oneidentity.com/products/identity-manager/ https://support.oneidentity.com/product-notification/noti-00001678
https://nvd.nist.gov/vuln/detail/CVE-2024-12649	9.8	Canon (Small Office Multifunction Printers and Laser Printers)	Out-of-bounds Write	Multiple products / versions	N/A	https://global.canon/en/index.html https://psirt.canon/advisory-information/cp2025-001/
https://nvd.nist.gov/vuln/detail/CVE-2024-57595	9.8	DLINK DIR-825	OS Command Injection	REVB 2.03	N/A	https://www.dlink.com/in/en/products/dir-825-ac1200-wifi-gigabit-router https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2024-55573	9.1	Centreon centreon-web	SQL Injection	24.10.x before 24.10.3, 24.04.x before 24.04.9, 23.10.x before 23.10.19, 23.04.x before 23.04.24	N/A	https://www.centreon.com/ https://github.com/centreon/centreon/releases https://thewatch.centreon.com/latest-security-bulletins-64/cve-2024-55573-centreon-web-critical-severity-4264
https://nvd.nist.gov/vuln/detail/CVE-2025-22604	9.1	Cacti (open source performance and fault management framework)	OS Command Injection	N/A	1.2.29	https://www.cacti.net/ https://github.com/Cacti/cacti/security/advisories/GHSA-c5j8-jxj3-hh36
https://nvd.nist.gov/vuln/detail/CVE-2022-4975	8.9	Red Hat Advanced Cluster Security	Cross-site Scripting	N/A	N/A	https://www.redhat.com/en/technologies/cloud-computing/openshift/advanced-cluster-security-kubernetes https://access.redhat.com/security/cve/CVE-2022-4975

https://nvd.nist.gov/vuln/detail/CVE-2024-39750	8.8	IBM Analytics Content Hub	Improper Restriction of Operations	2	N/A	https://community.ibm.com/community/user/businessanalytics/viewdocument/analytics-content-hub https://www.ibm.com/support/pages/node/7172787
https://nvd.nist.gov/vuln/detail/CVE-2024-41739	8.8	IBM Cognos Dashboards	Uncontrolled Search Path Element	4.0.7 and 5.0.0	N/A	https://www.ibm.com/docs/en/cognos-analytics/11.1.0?topic=dashboards-cognos-analytics-tutorial https://www.ibm.com/support/pages/node/7177766
https://nvd.nist.gov/vuln/detail/CVE-2025-0314	8.7	GitLab CE/EE	Cross-site Scripting	all versions from 17.2 before 17.6.4, 17.7 before 17.7.3, and 17.8 before 17.8.1	N/A	https://about.gitlab.com/install/ce-or-ee/ https://gitlab.com/gitlab-org/gitlab/-/issues/512118
https://nvd.nist.gov/vuln/detail/CVE-2024-9493	8.6	ToolStick installer (SILABS)	Uncontrolled Search Path Element	N/A	N/A	https://www.silabs.com/development-tools/mcu/8-bit/mcu-university-toolstick-kit?tab=overview https://community.silabs.com/068Vm00000JUQwd
https://nvd.nist.gov/vuln/detail/CVE-2024-9495	8.6	CP210x VCP Windows installer (SILABS)	Uncontrolled Search Path Element	N/A	N/A	https://www.silabs.com/developer-tools/usb-to-uart-bridge-vcp-drivers https://community.silabs.com/068Vm00000JUQwd
https://nvd.nist.gov/vuln/detail/CVE-2024-9497	8.6	USBXpress 4 SDK installer (SILABS)	Uncontrolled Search Path Element	N/A	N/A	https://www.silabs.com/interface/usb-bridges https://community.silabs.com/068Vm00000JUQwd
https://nvd.nist.gov/vuln/detail/CVE-2025-23222	8.4	Deepin dde-api-proxy	Improper Verification of Source of a Communication Channel	through 1.0.19	N/A	https://security.opensuse.org/2025/01/24/dde-api-proxy-privilege-escalation.html https://bugzilla.suse.com/show_bug.cgi?id=1229918
https://nvd.nist.gov/vuln/detail/CVE-2022-49043	8.1	libxml2	Use After Free	before 2.11.0	N/A	https://en.wikipedia.org/wiki/Libxml2 https://github.com/php/php-src/issues/17467
https://nvd.nist.gov/vuln/detail/CVE-2024-40693	8	IBM Planning Analytics	Unrestricted Upload of File with Dangerous Type	2.0 and 2.1	N/A	https://www.ibm.com/products/planning-analytics https://www.ibm.com/support/pages/node/7168387
https://nvd.nist.gov/vuln/detail/CVE-2025-0543	7.8	G DATA Security Client	Incorrect Default Permissions	N/A	N/A	https://www.gdatasoftware.com/downloads https://github.com/nullby73/security-advisories/tree/main/CVE-2025-0543
https://nvd.nist.gov/vuln/detail/CVE-2024-53588	7.8	iTop VPN	Uncontrolled Search Path Element	v16.0	N/A	https://www.itopvpn.com/ https://github.com/JonathanLauener/iTop-privesc
https://nvd.nist.gov/vuln/detail/CVE-2025-0065	7.8	TeamViewer Clients	Argument Injection	prior version 15.62 for Windows	N/A	https://www.teamviewer.com https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2025-1001/
https://nvd.nist.gov/vuln/detail/CVE-2024-0146	7.8	NVIDIA vGPU	Classic Buffer Overflow	N/A	N/A	https://www.nvidia.com/en-eu/geforce/graphics-cards/ https://nvidia.custhelp.com/app/answers/detail/a_id/5614

https://nvd.nist.gov/vuln/detail/CVE-2024-13562	7.5	Import WP – Export and Import CSV and XML files to WordPress	Exposure of Sensitive Information	all versions up to, and including, 2.14.5	N/A	https://wordpress.org/plugins/jc-importer/ https://www.wordfence.com/threat-intel/vulnerabilities/id/d6d69ffd-bb39-4fcc-9444-27d1a901e7c9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-12600	7.2	Custom Product Tabs Lite for WooCommerce plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 1.9.0	N/A	https://wordpress.org/plugins/woocommerce-custom-product-tabs-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/33c16b47-3202-4f26-bf45-98172b8cac45?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-13509	7.2	WS Form LITE – Drag & Drop Contact Form Builder for WordPress	Cross-site Scripting	all versions up to, and including, 1.10.13	N/A	https://wordpress.org/plugins/ws-form/ https://www.wordfence.com/threat-intel/vulnerabilities/id/910d9b31-b63a-427e-830b-a4c6a7e77ade?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-0411	7	7-Zip	Protection Mechanism Failure	N/A	N/A	https://www.7-zip.org/ http://www.openwall.com/lists/oss-security/2025/01/24/6 https://www.zerodayinitiative.com/advisories/ZDI-25-045/

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Known Exploited Vulnerability to Catalog	CVE-2025-23006 SonicWall SMA1000 Appliances Deserialization Vulnerability	https://www.cisa.gov/news-events/alerts/2025/01/24/cisa-adds-one-known-exploited-vulnerability-catalog

3 News

Σύντομη περιγραφή / Τίτλος	URL
THN Weekly Recap: Top Cybersecurity Threats, Tools and Tips [27 January]	https://thehackernews.com/2025/01/thn-weekly-recap-top-cybersecurity_27.html
SECURITY AFFAIRS MALWARE NEWSLETTER – ROUND 30	https://securityaffairs.com/173461/malware/security-affairs-malware-newsletter-round-30.html
This Week In Cybersecurity: 20th January to 24th January	https://dailysecurityreview.com/security-spotlight/this-week-in-cybersecurity-20th-january-to-24th-january/
Hacker infects 18,000 "script kiddies" with fake malware builder	https://www.bleepingcomputer.com/news/security/hacker-infects-18-000-script-kiddies-with-fake-malware-builder/
Chinese AI platform DeepSeek faced a “large-scale” cyberattack	https://securityaffairs.com/173546/security/chinese-ai-platform-deepseek-faced-a-large-scale-cyberattack.html
Weekly Cybersecurity Update: Recent Cyber Attacks, Vulnerabilities, and Data Breaches	https://cybersecuritynews.com/weekly-cybersecurity-update-jan/

3.1 Breaches

Σύντομη περιγραφή / Τίτλος	URL
Change Healthcare data breach exposed the private data of over half the U.S.	https://securityaffairs.com/173467/data-breach/change-healthcare-data-breach-190m-people.html
Over Six Million Hit by Ransomware Breach at Infosys McCamish Systems	https://www.infosecurity-magazine.com/news/six-million-ransomware-breach/
TalkTalk confirms data breach involving a third-party platform	https://securityaffairs.com/173526/cyber-crime/talktalk-confirms-data-breach.html

3.2 Vulnerabilities and flaws

Σύντομη περιγραφή / Τίτλος	URL
Most online Exchange Servers vulnerable to ProxyLogon still not remediated	https://www.scworld.com/brief/most-online-exchange-servers-vulnerable-to-proxylogon-still-not-remediated
Critical Fleet Server Vulnerability Exposes Sensitive Information	https://cybersecuritynews.com/critical-fleet-server-vulnerability/

Apache Solr For Windows Vulnerability Allows Arbitrary Path write-access	https://cybersecuritynews.com/apache-solr-arbitrary-path-write-access/
5,000+ SonicWall firewalls still open to attack (CVE-2024-53704)	https://www.helpnetsecurity.com/2025/01/27/5000-sonicwall-firewalls-still-open-to-attack-vulnerability-cve-2024-53704/
New Docker 1-Click RCE Attack Exploits Misconfigured API Settings	https://cybersecuritynews.com/docker-1-click-rce-attack/
FortiOS Authentication Bypass Vulnerability Exploited to Gain Super-Admin Access	https://cybersecuritynews.com/fortios-auth-bypass-vulnerability-exploited/

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Zyxel warns of bad signature update causing firewall boot loops	https://www.bleepingcomputer.com/news/security/zyxel-warns-of-bad-signature-update-causing-firewall-boot-loops/
Apple addressed the first zero-day vulnerability of 2025, which is actively exploited in attacks in the wild aimed at iPhone users.	https://securityaffairs.com/173536/hacking/apple-fixed-the-first-zero-day-vulnerability-of-2025.html
Apple Patches Actively Exploited Zero-Day Affecting iPhones, Macs, and More	https://thehackernews.com/2025/01/apple-patches-actively-exploited-zero.html
Chrome Security Update – Memory Corruption & Access Vulnerabilities Patched	https://cybersecuritynews.com/memory-corruption-access-vulnerabilities-patched/
GitLab Security Update – Patch for XSS Vulnerability in File Rendering	https://cybersecuritynews.com/patch-for-xss-vulnerability-in-file-rendering/

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
New Phishing Campaign Targets Mobile Devices with Malicious PDFs	https://www.infosecurity-magazine.com/news/phishing-campaign-targets-mobile/
GamaCopy targets Russia mimicking Russia-linked Gamaredon APT	https://securityaffairs.com/173501/apt/gamacopy-mimics-russia-linked-gamaredon-apt.html
ESXi ransomware attacks use SSH tunnels to avoid detection	https://securityaffairs.com/173487/cyber-crime/esxi-ransomware-attacks-use-ssh-tunnels-to-avoid-detection.html
Cisco warns of a ClamAV bug with PoC exploit	https://securityaffairs.com/173446/uncategorized/cisco-fixed-clamav-dos-flaw.html
IDOR on Tesla Disclosing Users' Emails	https://medium.com/@lonewolfx1/idor-on-tesla-disclosing-users-emails-9ea53380a315
Attacks on Ivanti appliances demonstrate danger of chained exploits	https://www.scworld.com/news/attacks-on-ivanti-appliances-demonstrate-danger-of-chained-exploits
SQL injection in largest Electricity Board of Sri Lanka	https://infosecwriteups.com/sql-injection-in-largest-electricity-board-of-sri-lanka-1a55c12104bd
New TorNet backdoor seen in widespread campaign	https://blog.talosintelligence.com/new-tornet-backdoor-campaign/
Royal Mail SMS Phishing Scam Targets Victims with Fake Delivery Fee Requests	https://hackread.com/royal-mail-sms-phishing-scam-fake-delivery-fee-requests/
New Malware Campaign Using 7z & UltraVNC Tool To Deploy Malware	https://cybersecuritynews.com/new-malware-campaign-using-7z-ultravnc-tool/

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Don’t let these open-source cybersecurity tools slip under your radar	https://www.helpnetsecurity.com/2025/01/27/open-source-cybersecurity-tools-free/
Top 10 Best Open Source Firewall in 2025	https://cybersecuritynews.com/best-open-source-firewall/
Stratoshark – Wireshark Has Got a Friend for Cloud	https://cybersecuritynews.com/stratoshark/
SCAVY – Framework to Detect Memory Corruption in Linux Kernel for Privilege Escalation	https://cybersecuritynews.com/detecting-memory-corruption-in-linux-kernel/
10 Best Vulnerability Assessment and Penetration Testing (VAPT) Tools in 2025	https://cybersecuritynews.com/best-vapt-tools/

4 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.

5 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/