Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 31/012024 - 04/02/2025

Contents

1 Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv 3	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-2025-21524	9.8	Oracle JD Edwards	allows unauthenticated attacker with network access via HTTP to compromise the system	Prior to 9.2.9.0	N/A	https://www.oracle.com/applications/jd-edwards-enterpriseone/ https://www.oracle.com/security-alerts/cpujan2025.html
https://nvd.nist.gov/vuln/detail/CVE-2024-57726	9.9	SimpleHelp remote support software	escalation of privileges	v5.5.7 and before	N/A	https://simple-help.com/ https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier
https://nvd.nist.gov/vuln/detail/CVE-2024-57968	9.9	Advantive VeraCore	Unrestricted Upload of File with Dangerous Type	before 2024.4.2.1	4.9.1	https://www.advantive.com/brands/veracore/ https://advantive.my.site.com/support/s/article/VeraCore-Release-Notes-2024-4-2-1 https://intezer.com/blog/research/xe-group-exploiting-zero-days/
https://nvd.nist.gov/vuln/detail/CVE-2023-28769	9.8	Zyxel DX5401-B0	buffer overflow	firmware versions prior to V5.17(ABYO.1)C0	N/A	https://www.zyxel.com/service-provider/global/en/products/dsl-cpe/vdsl/dx5401ex5401-b-series https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-0929	9.8	TeamCal Neo	SQL Injection	3.8.2	N/A	https://teamcalneo.lewe.com/ https://www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-teamcal-neo
https://nvd.nist.gov/vuln/detail/CVE-2024-45569	9.8	Qualcomm (WLAN)	Improper Validation of Array Index	N/A	N/A	https://www.qualcomm.com/ https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html
https://nvd.nist.gov/vuln/detail/CVE-2025-20634	9.8	Mediatek chipsets	Out-of-bounds Write	N/A	Patch ID: MOLY01289384; Issue ID: MSV-2436	https://www.mediatek.com/ https://corp.mediatek.com/product-security-bulletin/February-2025
https://nvd.nist.gov/vuln/detail/CVE-2025-0366	8.8	Jupiter X Core plugin for WordPress	PHP Remote File Inclusion	all versions up to, and including, 4.8.7	N/A	https://wordpress.org/plugins/jupiterx-core/ https://www.wordfence.com/threat-

						intel/vulnerabilities/id/1a20dc1d-eb7c-47ac-ad9a-ec4c0d5db62e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-53295	7.8	Dell PowerProtect DD	Insufficient Granularity of Access Control	prior to 8.3.0.0, 7.10.1.50, and 7.13.1.20	N/A	https://www.dell.com/en-us/dt/data-protection/powerprotect-backup-dd-appliances/powerprotect-dd-backup-appliances.htm https://www.dell.com/support/kbdoc/en-us/000279157/dsa-2025-022-security-update-for-dell-powerprotect-dd-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-35177	7.8	Wazuh	Improper Access Control	N/A	4.9.0	https://wazuh.com/ https://github.com/wazuh/wazuh/security/advisories/GHSA-pmr2-2r83-h3cv
https://nvd.nist.gov/vuln/detail/CVE-2025-0015	7.8	Arm Ltd Valhall GPU Kernel Driver,	Use After Free	Arm 5th Gen GPU	N/A	https://developer.arm.com/downloads/-/mali-drivers/valhall-kernel https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-12511	7.6	Xerox Versalink products	Improper Privilege Management	N/A	N/A	https://www.xerox.com/en-us/office https://securitydocs.business.xerox.com/wp-content/uploads/2025/02/Xerox-Security-Bulletin-XRX25-003-for-Xerox%C2%AE-for-VersaLinkPhaser-and-WorkCentre.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-45650	7.5	IBM Security Verify Directory	Improper Check for Unusual or Exceptional Conditions	10.0 through 10.0.3	N/A	https://www.ibm.com/docs/en/svd/10.0.2?topic=overview-security-verify-directory https://www.ibm.com/support/pages/node/7182169
https://nvd.nist.gov/vuln/detail/CVE-2024-10238	7.2	Supermicro MBD-X12DPG-OA6	Stack-based Buffer Overflow	N/A	N/A	https://www.supermicro.com/en/products/motherboard/x12dpg-oa6 https://www.supermicro.com/en/support/security_BMC_IPMI_Jan_2025
https://nvd.nist.gov/vuln/detail/CVE-2025-24830	7	Acronis Cyber Protect Cloud Agent	Untrusted Search Path	before build 39378	N/A	https://www.acronis.com/en-eu/products/cloud/cyber-protect https://security-advisory.acronis.com/advisories/SEC-7829
https://nvd.nist.gov/vuln/detail/CVE-2025-20890	7	Samsung mobile	Out-of-bounds write	SMR Jan-2025 Release 1	N/A	https://security.samsungmobile.com/main.smsb https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Vulnerability Summary for the Week of January 27, 2025	Common Vulnerabilities and Exposures (CVE)	https://www.cisa.gov/news-events/bulletins/sb25-034

3 News

Σύντομη περιγραφή / Τίτλος	URL
768 CVEs Exploited in 2024, Reflecting a 20% Increase from 639 in 2023	https://thehackernews.com/2025/02/768-cves-exploited-in-2024-reflecting.html
Weekly Cybersecurity Update: Recent Cyber Attacks, Vulnerabilities, and Data Breaches	https://cybersecuritynews.com/weekly-cybersecurity-update-jan-last-week/
THN Weekly Recap: Top Cybersecurity Threats, Tools and Tips [3 February]	https://thehackernews.com/2025/02/thn-weekly-recap-top-cybersecurity.html

3.1 Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
GrubHub data breach impacts customers, drivers, and merchants	https://www.bleepingcomputer.com/news/security/grubhub-data-breach-impacts-customers-drivers-and-merchants/
Web Skimmer found on at least 17 websites, including Casio UK	https://securityaffairs.com/173797/malware/web-skimmer-casio-uks-site.html
Globe Life Ransomware Attack – 850,000+ Users Personal & Health Data Exposed	https://cybersecuritynews.com/globe-life-ransomware-attack/
TAG-124 Hacked 1000+ WordPress Sites To Embed Payloads	https://cybersecuritynews.com/tag-124-hacked-1000-wordpress-sites/

3.2 Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Russian Cybercrime Groups Exploiting 7-Zip Flaw to Bypass Windows MotW Protections	https://thehackernews.com/2025/02/russian-cybercrime-groups-exploiting-7.html

AMD SEV-SNP Vulnerability Allows Malicious Microcode Injection with Admin Access	https://thehackernews.com/2025/02/amd-sev-snp-vulnerability-allows.html
Yeti Forensic Platform Vulnerability Allows Attackers to Execute Remote Code	https://gbhackers.com/yeti-forensic-platform-vulnerability/
Hackers Exploiting 7-Zip Zero-Day Vulnerability to Deploy SmokeLoader Malware	https://cybersecuritynews.com/7-zip-zero-day-vulnerability-smokeloader-malware/
Roundcube XSS Vulnerability Let Attackers Inject Malicious Files	https://cybersecuritynews.com/roundcube-xss-vulnerability/
Apple Service Ticket Portal Vulnerability Exposes Millions of Users Data	https://cybersecuritynews.com/apple-service-ticket-portal-vulnerability/
Apache Cassandra Vulnerability Let Attackers Gain Access to the Data Centers Remotely	https://cybersecuritynews.com/apache-cassandra-vulnerability/
Multiple Dell PowerProtect Vulnerabilities Let Attackers Compromise System	https://cybersecuritynews.com/multiple-dell-powerprotect-vulnerabilities/
Critical Microsoft Accounts Authentication Bypass Vulnerability Let Attackers Gain Remote Access	https://cybersecuritynews.com/crtical-microsoft-accounts-authentication-bypass-vulnerability/
Cisco's Webex Chat Vulnerabilities Let Attackers Access Organizations Chat Histories	https://cybersecuritynews.com/ciscos-webex-chat-vulnerabilities/

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Google Patches 47 Android Security Flaws, Including Actively Exploited CVE-2024-53104	https://thehackernews.com/2025/02/google-patches-47-android-security.html
Microsoft Patches Critical Azure AI Face Service Vulnerability with CVSS 9.9 Score	https://thehackernews.com/2025/02/microsoft-patches-critical-azure-ai.html

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Coyote Banking Trojan targets Brazilian users, stealing data from 70+ financial apps and websites	https://securityaffairs.com/173818/malware/coyote-banking-trojan-targets-brazilian-users.html
North Korean Hackers Deploy FERRET Malware via Fake Job Interviews on macOS	https://thehackernews.com/2025/02/north-korean-hackers-deploy-ferret.html
Sophisticated Phishing Attack Bypasses Microsoft ADFS MFA	https://www.infosecurity-magazine.com/news/phishing-attack-bypasses-microsoft/

WhatsApp: Global spyware campaign conducted by Israeli firm	https://www.scworld.com/brief/whatsapp-global-spyware-campaign-conducted-by-israeli-firm
Hackers Exploit Public-facing Vulnerable IIS, Apache, SQL Servers to Attack Gov & Telcom Networks	https://cybersecuritynews.com/hackers-exploit-public-facing-vulnerable-iis-apache-sql-servers/

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
10 Best Web Application Firewall (WAF) – 2025	https://cybersecuritynews.com/web-application-firewall/
BadDNS: Open-source tool checks for subdomain takeovers	https://www.helpnetsecurity.com/2025/02/03/baddns-open-source-tool-check-domain-subdomain-takeover/
Testing SIEM Detections Against Ransomware Using PsExec	https://osintteam.blog/testing-siem-detections-against-ransomware-using-psexec-1963bcb0cf3b
Parrot 6.3 Released With Improved Security & New Hacking Tools	https://cybersecuritynews.com/parrot-6-3-released/

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/