Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 17/012024 - 21/01/2025

Contents

1 Common Vulnerabilities and Exposures (CVE)

CVEs						
URL ευπάθειας (NIST NVD)	**CVS Sv3**	**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-2024-11639	**10**	Ivanti CSA	authentication bypass	before 5.0.3	N/A	https://help.ivanti.com/ld/help/en_US/LDMS/10.0/Windows/csa-h-help.htm https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Services-Application-CSA-CVE-2024-11639-CVE-2024-11772-CVE-2024-11773
https://nvd.nist.gov/vuln/detail/CVE-2024-41783	**9.1**	IBM Sterling Secure Proxy	os command injection	6.0.0.0, 6.0.0.1, 6.0.0.2, 6.0.0.3, 6.1.0.0, and 6.2.0.0	N/A	https://www.ibm.com/products/secure-proxy https://www.ibm.com/support/pages/node/7176189
https://nvd.nist.gov/vuln/detail/CVE-2024-11005	**9.1**	Ivanti Connect Secure & Ivanti Policy Secure	remote code execution	before version 22.7R2.1 (Not Applicable to 9.1Rx) & before version 22.7R1.1 (Not Applicable to 9.1Rx)	N/A	https://www.ivanti.com/products/connect-secure-vpn https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs
https://nvd.nist.gov/vuln/detail/CVE-2025-0566	**8.8**	Tenda AC15	Improper Restriction of Operations within the Bounds of a Memory Buffer	15.13.07.13	N/A	https://www.smallnetbuilder.com/wireless/wireless-reviews/tenda-ac15-ac1900-smart-dual-band-gigabit-wifi-router-reviewed/ https://vuldb.com/?submit.484418
https://nvd.nist.gov/vuln/detail/CVE-2023-50739	**8.8**	Lexmark devices	Heap-based Buffer Overflow	N/A	N/A	https://www.lexmark.com/en_US/products/series/printer-and-multifunction/finder.shtml https://www.lexmark.com/en_us/solutions/security/lexmark-security-advisories.html

https://nvd.nist.gov/vuln/detail/CVE-2024-10497	8.8	Schneider Electric devices	Authorization Bypass Through User-Controlled Key	N/A	N/A	https://www.se.com/ww/en/ https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-014-08&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-014-08.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-27894	8.5	Pulsar Functions Worker (Apache)	Unauthorized File Access and Unauthorized HTTP/HTTPS Proxyin	2.4.0 to 2.10.5, from 2.11.0 to 2.11.3, from 3.0.0 to 3.0.2, from 3.1.0 to 3.1.2, and 3.2.0. 2.10	at least 2.10.6. 2.11 at least 2.11.4. 3.0 at least 3.0.3. 3.1 at least 3.1.3. 3.2 at least 3.2.1	https://pulsar.apache.org/docs/2.10.x/functions-worker/ https://pulsar.apache.org/security/CVE-2024-27894/
https://nvd.nist.gov/vuln/detail/CVE-2024-47113	8.1	IBM ICP - Voice Gateway	XML Injection (aka Blind XPath Injection)	1.0.2, 1.0.2.4, 1.0.3, 1.0.4, 1.0.5, 1.0.6. 1.0.7, 1.0.7.1, and 1.0.8	N/A	https://www.ibm.com/docs/ar/cloud-private/3.2.0?topic=paks-voice-gateway https://www.ibm.com/support/pages/node/7175791
https://nvd.nist.gov/vuln/detail/CVE-2024-41743	7.5	IBM TXSeries for Multiplatforms	Allocation of Resources Without Limits or Throttling	N/A	N/A	https://www.ibm.com/products/txseries-for-multiplatforms https://www.ibm.com/support/pages/node/7172103
https://nvd.nist.gov/vuln/detail/CVE-2024-45662	7.5	IBM Safer Payments	Allocation of Resources Without Limits or Throttling	6.4.0.00 through 6.4.2.07, 6.5.0.00 through 6.5.0.05, and 6.6.0.00 through 6.6.0.03	N/A	https://www.ibm.com/products/safer-payments https://www.ibm.com/support/pages/node/7173765
https://nvd.nist.gov/vuln/detail/CVE-2025-0308	7.5	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership	SQL Injection	all versions up to, and including, 2.9.1	N/A	https://wordpress.org/plugins/ultimate-member/ https://www.wordfence.com/threat-intel/vulnerabilities/id/e3e5bb98-2652-499a-b8cd-4ebfe1c1d890?source=cve

		Plugin plugin for WordPress				
https://nvd.nist.gov/vuln/detail/CVE-2025-0355	7.5	NEC Corporation Aterm	Missing Authentication for Critical Function	multiple products / versions	N/A	https://www.nec.com/ https://jpn.nec.com/security-info/secinfo/nv25-003_en.html
https://nvd.nist.gov/vuln/detail/CVE-2025-21399	7.4	Microsoft Edge (Chromium-based)	Improper Check for Dropped Privileges	N/A	N/A	https://support.microsoft.com/en-us/microsoft-edge/download-the-new-microsoft-edge-based-on-chromium-0f4a3dd7-55df-60f5-739f-00010dba52cf https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21399
https://nvd.nist.gov/vuln/detail/CVE-2024-26153	7.4	ETIC Telecom Remote Access Server (	Cross-Site Request Forgery (CSRF)	prior to 4.9.19	N/A	https://www.etictelecom.com/en/machine-remote-maintenance/ https://www.cisa.gov/news-events/ics-advisories/icsa-22-307-01
https://nvd.nist.gov/vuln/detail/CVE-2025-0528	7.2	Tenda AC8	Improper Neutralization of Special Elements	AC8, AC10 and AC18 16.03.10.20	N/A	https://www.tendacn.com/product/overview/ac8.html https://github.com/Pr0b1em/IoT/blob/master/TendaAC10v16.03.10.20telnet.md
https://nvd.nist.gov/vuln/detail/CVE-2024-13377	7.2	Gravity Forms plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	all versions up to, and including, 2.9.1.3	N/A	https://www.gravityforms.com/ https://www.wordfence.com/threat-intel/vulnerabilities/id/03623f00-2c3c-4590-92fe-a5eaac15b944?source=cve

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
CISA and FBI Release Updated Guidance on Product Security Bad Practices	Cybersecurity Best Practices, Critical Infrastructure Security and Resilience	https://www.cisa.gov/news-events/alerts/2025/01/17/cisa-and-fbi-release-updated-guidance-product-security-bad-practices

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
Researchers Identify Principles to Reduce Noise in Network Intrusion Detection Systems in SOC	https://cybersecuritynews.com/network-intrusion-detection-systems-in-soc/
SECURITY AFFAIRS MALWARE NEWSLETTER – ROUND 29	https://securityaffairs.com/173232/malware/security-affairs-malware-newsletter-round-29.html
Weekly Cybersecurity Digest: Latest in Cyber Attacks, Vulnerabilities, & Data Breaches	https://cybersecuritynews.com/weekly-cybersecurity-digest/
Experts found multiple flaws in Mercedes-Benz infotainment system	https://securityaffairs.com/173275/hacking/mercedes-benz-infotainment-system-flaws.html
Microsoft shares temp fix for Outlook crashing when writing emails	https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-temp-fix-for-outlook-crashing-when-writing-emails/
THN Weekly Recap: Top Cybersecurity Threats, Tools and Tips [20 January]	https://thehackernews.com/2025/01/thn-weekly-recap-top-cybersecurity_20.html

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Hackers Allegedly Claiming Breach Of Hewlett Packard Enterprise	https://cybersecuritynews.com/hackers-alleged-hewlett-packard-breach/
HPE Data Breached by IntelBroker: HPE Data on Sale on Dark Web	https://dailysecurityreview.com/security-spotlight/hpe-data-breached-by-intelbroker-hpe-data-on-sale-on-dark-web/
Otelier Data Breach Exposes Millions of Hotel Reservations and Personal Information	https://dailysecurityreview.com/security-spotlight/otelier-data-breach-exposes-millions-of-hotel-reservations-and-personal-information/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Planet WGS-804HPT Industrial Switch flaws could be chained to achieve remote code execution	https://securityaffairs.com/173237/security/wgs-804hpt-flaws.html
PoC Exploit Released For QNAP Remote Code Execution Vulnerability	https://cybersecuritynews.com/qnap-rce-exploit-released/
HPE Aruba Network Vulnerabilities Let Attackers Execute Arbitrary Code Remotely	https://cybersecuritynews.com/hpe-aruba-network/
Windows Common Log File System Zero-day Vulnerability (CVE-2024-49138) Exploited	https://cybersecuritynews.com/clfs-zero-day-cve-2024-49138/
Windows 11 BitLocker-Encrypted Files Accessed Without Disassembling Laptops	https://cybersecuritynews.com/windows-11-bitlocker-encrypted-files-accessed/
PoC Released For Ivanti Connect Secure RCE Vulnerability (CVE-2025-0282)	https://cybersecuritynews.com/new-poc-released-for-ivanti-connect-secure-rce/
Vim Command Line Text Editor Vulnerability Tiggers Potential Crash	https://cybersecuritynews.com/vim-vulnerability-binary/
OpenVPN Easy-RSA Vulnerability Enables Bruteforce of Private CA Key	https://cybersecuritynews.com/openvpn-easy-rsa-vulnerability/
TP-Link Router Buffer Overflow Vulnerability Exploited to Execute Code	https://cybersecuritynews.com/tp-link-router-buffer-overflow-vulnerability/
7-Zip Vulnerability Let Remote Attackers Bypass Protections & Execute Arbitrary Code	https://cybersecuritynews.com/7-zip-vulnerability-arbitrary-code-2/
Critical Injection Vulnerability in SUSE Linux Distro Let Attackers Exploits “go-git” Library	https://cybersecuritynews.com/critical-injection-vulnerability-in-suse-linux-distro/
Microsoft fixes Windows Server 2022 bug breaking device boot	https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-server-2022-bug-breaking-device-boot/
126 Linux kernel Vulnerabilities Lets Attackers Exploit 78 Linux Sub-Systems	https://cybersecuritynews.com/126-linux-kernel-vulnerabilities/
New UEFI vulnerability bypasses Secure Boot — bootkits stay undetected even after OS re-install	https://www.tomshardware.com/pc-components/motherboards/new-uefi-vulnerability-bypasses-secure-boot-bootkits-stay-undetected-even-after-os-re-install

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
How Russian hackers went after NGOs' WhatsApp accounts	https://www.helpnetsecurity.com/2025/01/17/star-blizzard-whatsapp-phishing-ngos/
New Android Malware Mimics Chat App to Steal Sensitive Data	https://cybersecuritynews.com/new-android-malware-mimics-chat-app/
CERT-UA Warns of Cyber Scams Using Fake AnyDesk Requests for Fraudulent Security Audits	https://thehackernews.com/2025/01/cert-ua-warns-of-cyber-scams-using-fake.html
New Android Malware Mimics Chat App to Steal Sensitive Data	https://cybersecuritynews.com/new-android-malware-mimics-chat-app/
PNGPlug Loader Delivers ValleyRAT Malware Through Fake Software Installers	https://thehackernews.com/2025/01/pngplug-loader-delivers-valleyrat.html
New IoT Botnet Launching Large-Scale DDoS Attacks Hijacking IoT Devices	https://cybersecuritynews.com/new-iot-botnet-launching-large-scale-ddos-attacks/
ChatGPT Crawler Vulnerability Let Attackers Trigger DDoS Attack On Any Websites	https://cybersecuritynews.com/chatgpt-crawler-vulnerability/
DoNot Team Linked to New Tanzeem Android Malware Targeting Intelligence Collection	https://thehackernews.com/2025/01/donot-team-linked-to-new-tanzeem.html

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Fleet: Open-source platform for IT and security teams	https://www.helpnetsecurity.com/2025/01/21/fleet-open-source-platform-it-security-teams/
Splunk Series: Installation Guide for Windows and Linux (Part 1)	https://infosecwriteups.com/splunk-series-installation-guide-for-windows-and-linux-part-1-97a42f067c73

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/