Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/04/2025 - 08/04/2025

Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-25000	8,8	Microsoft Edge (Chromium-based	Access of Resource Using Incompatible Type ('Type Confusion')	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-25000
https://nvd.nist.gov/vuln/detail/CVE-2024-45199	8,8	insightsoftware Hive JDBC	Improper Control of Generation of Code ('Code Injection')	insightsoftware Hive JDBC through 2.6.13	https://gist.github.com/azraelxuemo/d019ad079d540ef28870dbd9552a7c62
https://nvd.nist.gov/vuln/detail/CVE-2025-3346	8,8	Tenda AC7	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Tenda AC7 15.03.06.44	https://github.com/CH13hh/tmp_store_cc/blob/main/AC7formSetPPTPServer/formSetPPTPServer.md https://vuldb.com/?ctiid.303560 https://vuldb.com/?id.303560 https://vuldb.com/?submit.551927 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2024-43067	7,8	EEPROM	Time-of-check Time-of-use (TOCTOU) Race Condition	Memory corruption occurs during the copying of read data from the EEPROM because the IO configuration is exposed as shared memory.	https://docs.qualcomm.com/product/publicresources/securitybulletin/april-2025-bulletin.html
https://nvd.nist.gov/vuln/detail/CVE-2025-29815	7,6	Microsoft Edge (Chromium-based)	Use After Free	Use after free in Microsoft Edge (Chromium-based) allows an authorized attacker to execute code over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29815

https://nvd.nist.gov/vuln/detail/CVE-2024-47213	7,5	Enrich	Improper Resource Shutdown or Release	Enrich 5.1.0 and below	https://support.snowplow.io/hc/en-us/articles/26318139354909-Update-Critical-Snowplow-Security-Updates-Impact-on-Open-Source-Software-Users
https://nvd.nist.gov/vuln/detail/CVE-2024-47212	7,5	Iglu Server	Uncontrolled Resource Consumption	Iglu Server 0.13.0 and below	https://support.snowplow.io/hc/en-us/articles/26318139354909-Update-Critical-Snowplow-Security-Updates-Impact-on-Open-Source-Software-Users
https://nvd.nist.gov/vuln/detail/CVE-2025-30370	7,4	jupyterlab-git is a JupyterLab extension for version control using Git	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	On many platforms, a third party can create a Git repository under a name that includes a shell command substitution string in the syntax $(command).	https://github.com/jupyterlab/jupyterlab-git/blob/7eb3b06f0092223bd5494688ec264527bbeb2195/src/commandsAndMenu.tsx#L175-L184 https://github.com/jupyterlab/jupyterlab-git/commit/b46482993f76d3a546015c6a94ebed8b77fc2376 https://github.com/jupyterlab/jupyterlab-git/pull/1196 https://github.com/jupyterlab/jupyterlab-git/security/advisories/GHSA-cj5w-8mjf-r5f8 https://github.com/jupyterlab/jupyterlab-git/security/advisories/GHSA-cj5w-8mjf-r5f8
https://nvd.nist.gov/vuln/detail/CVE-2025-3401	7,3	ESAFENET CDG	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	ESAFENET CDG 5.6.3.154.205_20250114	https://github.com/Rain1er/report/blob/main/CDG/Ng%3D%3D.md https://vuldb.com/?ctiid.303646 https://vuldb.com/?id.303646 https://vuldb.com/?submit.525612

https://nvd.nist.gov/vuln/detail/CVE-2025-3379	7,3	PCMan FTP Server	uffer Copy without Checking Size of Input ('Classic Buffer Over-flow')	PCMan FTP Server 2.0.7	https://fitoxs.com/exploit/exploit-bb0f6aa46681315f8c62a944a52a3f4e.txt https://fitoxs.com/exploit/exploit-bb0f6aa46681315f8c62a944a52a3f4e.txt https://vuldb.com/?ctiid.303625 https://vuldb.com/?id.303625 https://vuldb.com/?submit.552341
https://nvd.nist.gov/vuln/detail/CVE-2024-43065	7,1	Cryptographic issues	Exposed Dangerous Method or Function	Cryptographic issues while generating an asymmetric key pair for RKP use cases.	https://docs.qualcomm.com/product/publicre-sources/securitybulletin/april-2025-bulletin.html

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	**CVE-2025-31161**	https://www.cisa.gov/news-events/alerts/2025/04/07/cisa-adds-one-known-exploited-vulnerability-catalog
Ivanti Releases Security Updates for Connect Secure, Policy Secure & ZTA Gateways Vulnerability (CVE-2025-22457)	**CVE-2025-22457**	https://www.cisa.gov/news-events/alerts/2025/04/04/ivanti-releases-security-updates-connect-secure-policy-secure-zta-gateways-vulnerability-cve-2025
CISA Adds One Vulnerability to the KEV Catalog	**CVE-2025-22457**	https://www.cisa.gov/news-events/alerts/2025/04/04/cisa-adds-one-vulnerability-kev-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
CISA Releases NICE Workforce Framework Version 2.0.0 Released – What's New	https://cybersecuritynews.com/nice-workforce-framework-version-2-0-0-released/
Cybersecurity Weekly Recap: Key Updates on Attacks, Vulnerabilities, & Data Breaches	https://cybersecuritynews.com/cybersecurity-weekly-recap-key-updates/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
50,000+ WordPress Sites Vulnerable to Privilege Escalation Attacks	https://cybersecuritynews.com/50000-wordpress-sites-vulnerable/
CISA Adds Actively Exploits Ivanti Connect Secure Vulnerability in Known Exploited Catalog	https://cybersecuritynews.com/cisa-adds-actively-exploits-ivanti-connect-secure-vulnerability/
React Router Flaw Exposes Web Apps to Cache Poisoning & WAF Bypass Attacks	https://cybersecuritynews.com/react-router-vulnerability-exposes-web-apps/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Hackers Exploiting Windows .RDP Files For Rogue Remote Desktop Connections	https://cybersecuritynews.com/hackers-exploiting-windows-rdp-files-for-rogue-remote-desktop-connections/
Threat Actors Weaponize Windows Screensavers Files to Deliver Malware	https://cybersecuritynews.com/threat-actors-weaponize-windows-screensavers-files-to-deliver-malware/
ToddyCat Hackers Exploit ESET's Command Line Scanner Vulnerability to Evade Detection	https://cybersecuritynews.com/toddycat-attackers-exploited-eset-command-line-scanner-vulnerability/
Threat Actors Using Fake CAPTCHAs and CloudFlare Turnstile to Deliver LegionLoader	https://cybersecuritynews.com/fake-captchas-cloudflare-turnstile-legionloader/
NEPTUNE RAT Attacking Windows Users to Exfiltrate Passwords from 270+ Apps	https://cybersecuritynews.com/neptune-rat-attacking-windows-users/
Dell PowerProtect Systems Vulnerability Let Remote Attackers Execute Arbitrary Commands	https://cybersecuritynews.com/dell-powerprotect-systems-vulnerability/
Critical pgAdmin Vulnerability Let Attackers Execute Remote Code	https://cybersecuritynews.com/critical-pgadmin-vulnerability/
Bitdefender GravityZone Console PHP Vulnerability Let Attackers Execute Arbitrary Commands	https://cybersecuritynews.com/bitdefender-gravityzone-console-flaw/
"Clipboard Hijacking" A Fake CAPTCHA Leverage Pastejacking Script Via Hacked Sites To Steal Clipboard Data	https://cybersecuritynews.com/fake-captcha/
New Android Spyware That Asks Password From Users to Uninstall	https://cybersecuritynews.com/android-spyware-asks-password-to-uninstall/
New Credit Card Skimming Attack Leverages Chrome, Edge, & Firefox Extensions to Steal Financial Data	https://cybersecuritynews.com/new-credit-card-skimming-attack/
Chinese Hackers Actively Exploiting Ivanti VPN Vulnerability to Deploy Malware	https://cybersecuritynews.com/chinese-hackers-actively-exploiting-ivanti-vpn-vulnerability/
OpenVPN Vulnerability Let Attackers Crash Servers & Execute Remote Code	https://cybersecuritynews.com/openvpn-vulnerability-let-attackers-crash-servers/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
MediaTek Security Update – Patch for Vulnerabilities Affecting Smartphone, Tablet, & other Devices	https://cybersecuritynews.com/mediatek-security-update-patch-for-vulnerabilities/
Microsoft Strengthens Outlook's Email Ecosystem to Protect Inboxes	https://cybersecuritynews.com/microsoft-strengthens-outlook/
Ivanti Connect Secure RCE Vulnerability Actively Exploited in the Wild – Apply Patch Now!	https://cybersecuritynews.com/ivanti-connect-secure-vulnerability-actively-exploited-in-the-wild/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
10 Best Ransomware File Decryptor Tools – 2025	https://cybersecuritynews.com/ransomware-file-decryptor-tools/
30 Best Cyber Security Search Engines In 2025	https://cybersecuritynews.com/cyber-security-search-engines/
Top 20 Best Endpoint Management Tools – 2025	https://cybersecuritynews.com/endpoint-management-tools/
Top 10 Best Password Managers in 2025	https://cybersecuritynews.com/best-password-managers/
Frida Penetration Testing Tool Kit Released With New APIs for Threat Monitoring	https://cybersecuritynews.com/frida-penetration-testing-tool-kit-released/

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/