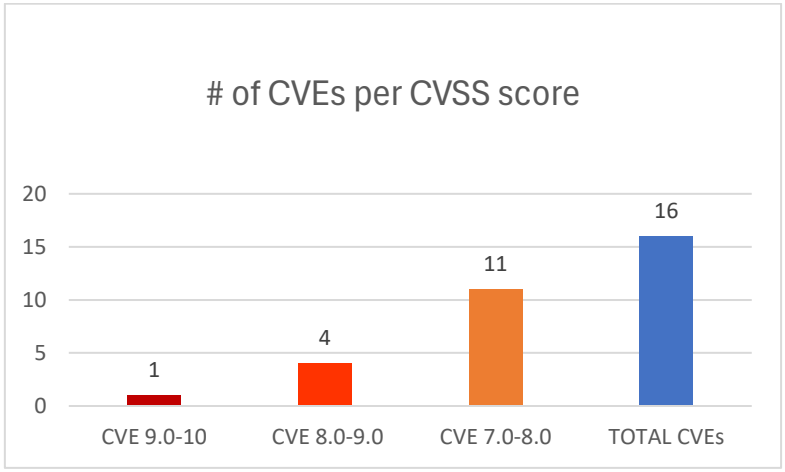
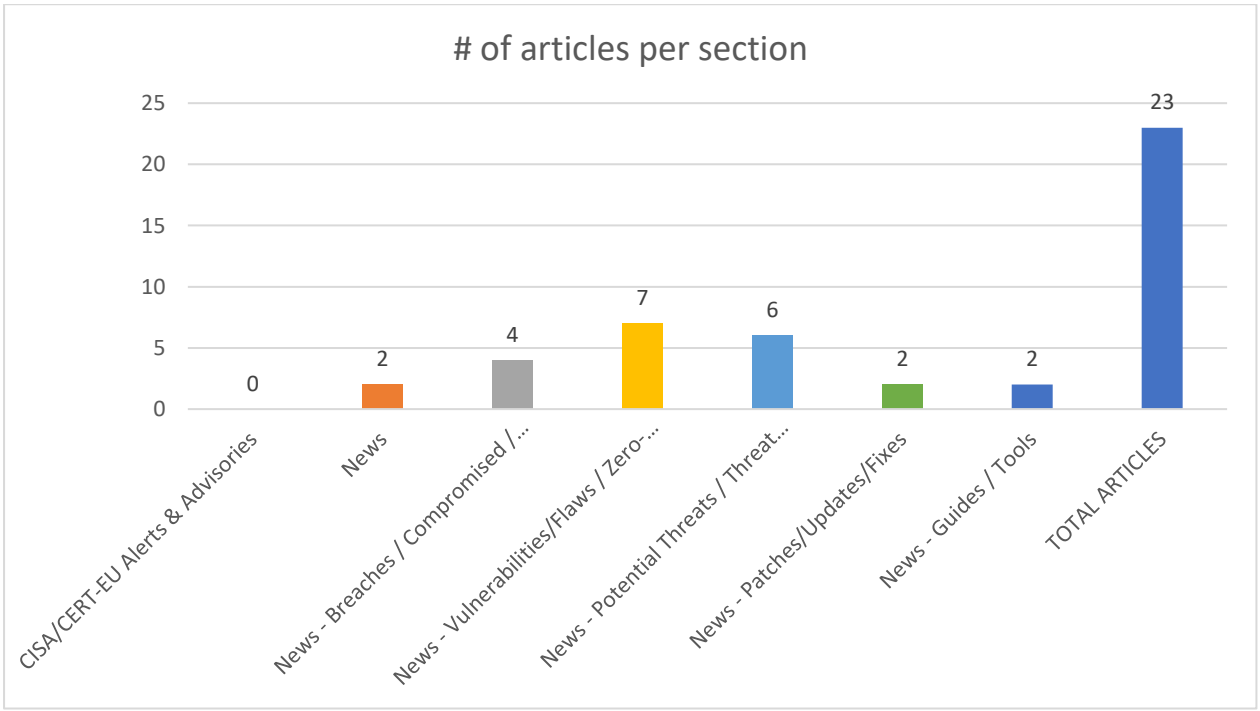
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 02/08/2025 - 05/08/2025





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-2025-7710	9,8	The Brave Conversion Engine (PRO) plugin for WordPress	Authentication Bypass Using an Alternate Path or Channel	all versions up to, and including, 0.7.7	https://getbrave.io/brave-pro-changelog/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/604249c6-b23a-40e9-984d-2014f5c97249?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54351	8,9	iperf	Unprotected Alternate Channel	before 3.19.1	https://github.com/esnet/iperf/commit/969b7f70c447513e92c9798f22e82b40ebc53bf0 MITRE https://github.com/esnet/iperf/releases/tag/3.19.1
https://nvd.nist.gov/vuln/detail/CVE-2025-6754	8,8	The SEO Metrics plugin for WordPress	Missing Authorization	versions 1.0.5 through 1.0.15	https://plugins.trac.wordpress.org/browser/seo-metrics-helper/trunk/common-functions.php Wordfence https://plugins.trac.wordpress.org/browser/seo-metrics-helper/trunk/endpoint.php Wordfence https://plugins.trac.wordpress.org/browser/seo-metrics-helper/trunk/seo-metrics.php Wordfence https://plugins.trac.wordpress.org/browser/seo-metrics-helper/trunk/welcome-page.php Wordfence https://wordpress.org/plugins/seo-metrics-helper/#developers Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/48658b33-ae53-4919-8180-1188f72553f7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54424	8,1	1Panel	Improper Neutralization of Special Elements used in a Command ('Command Injection')	versions 2.0.5 and below	https://github.com/1Panel-dev/1Panel/pull/9698/commits/4003284521f8d31ddaf7215d1c30ab8b4cdb0261 GitHub, Inc. https://github.com/1Panel-dev/1Panel/releases/tag/v2.0.6 GitHub, Inc. https://github.com/1Panel-dev/1Panel/security/advisories/GHSA-8j63-96wh-wh3j

https://nvd.nist.gov/vuln/detail/CVE-2025-54955	8,1	OpenNebula	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	Community Edition (CE) before 7.0.0 and Enterprise Edition (EE) before 6.10.3	https://docs.opennebula.io/6.10/intro_release_notes/release_notes_enterprise/resolved_issues_6103.html MITRE https://github.com/OpenNebula/one MITRE https://github.com/OpenNebula/one/commit/81058d9705e7ac619d294423de28b76d88f613b6 MITRE https://github.com/OpenNebula/one/releases/tag/release-7.0.0 MITRE https://github.com/Stolichnayer/OpenNebula-Account-Takeover
https://nvd.nist.gov/vuln/detail/CVE-2025-23276	7,8	NVIDIA Installer for Windows	Files or Directories Accessible to External Parties		https://nvidia.custhelp.com/app/answers/detail/a_id/5670
https://nvd.nist.gov/vuln/detail/CVE-2025-23283	7,8	NVIDIA vGPU software for Linux-style hypervisors	Stack-based Buffer Overflow		https://nvidia.custhelp.com/app/answers/detail/a_id/5670
https://nvd.nist.gov/vuln/detail/CVE-2025-54796	7,5	Copyparty	Uncontrolled Resource Consumption	Versions prior to 1.18.9	https://github.com/9001/copyparty/commit/09910ba80784c3980947d92f45db696398c0fd83 GitHub, Inc. https://github.com/9001/copyparty/releases/tag/v1.18.9 GitHub, Inc. https://github.com/9001/copyparty/security/advisories/GHSA-5662-2rj7-f2v6
https://nvd.nist.gov/vuln/detail/CVE-2025-8469	7,3	SourceCodester Online Hotel Reservation System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/K1nakoo/tmp01/blob/main/tmp01.md VulDB https://vuldb.com/?ctiid.318519 VulDB https://vuldb.com/?id.318519 VulDB https://vuldb.com/?submit.626017 VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-8468	7,3	Wazifa System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/wllovemy/cve/issues/13 VulDB https://vuldb.com/?ctiid.318518 VulDB https://vuldb.com/?id.318518 VulDB https://vuldb.com/?submit.625787

https://nvd.nist.gov/vuln/detail/CVE-2025-8466	7,3	Online Farm System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/wllovemy/cve/issues/11 VulDB https://vuldb.com/?ctiid.318516 VulDB https://vuldb.com/?id.318516 VulDB https://vuldb.com/?submit.625785
https://nvd.nist.gov/vuln/detail/CVE-2025-23277	7,3	NVIDIA Display Driver for Linux and Windows	Improper Access Control		https://https://nvidia.custhelp.com/app/answers/detail/a_id/5670
https://nvd.nist.gov/vuln/detail/CVE-2025-8471	7,3	Online Admission System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/tqlfront/CVE/issues/1 VulDB https://vuldb.com/?ctiid.318521 VulDB https://vuldb.com/?id.318521 VulDB https://vuldb.com/?submit.626115
https://nvd.nist.gov/vuln/detail/CVE-2025-8499	7,3	Online Medicine Guide	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/joker-vip/cvesubmit/issues/1 CISA-ADP, VulDB https://vuldb.com/?ctiid.318598 VulDB https://vuldb.com/?id.318598 VulDB https://vuldb.com/?submit.626778
https://nvd.nist.gov/vuln/detail/CVE-2025-8495	7,3	Membership Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://vuldb.com/?ctiid.318594 VulDB https://vuldb.com/?id.318594 VulDB https://vuldb.com/?submit.626722 VulDB https://www.yuque.com/gongzi-jsnek/xb2q3a/dctpzq93gcaop8qo?singleDoc
https://nvd.nist.gov/vuln/detail/CVE-2025-54136	7,2	Cursor	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	versions 1.2.4 and below	https://github.com/cursor/cursor/security/advisories/GHSA-24mc-g4xr-4395

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
-	-	-

News

Σύντομη περιγραφή / Τίτλος	URL
Hacking group D4rk4rmy claimed the hack of Monte-Carlo Société des Bains de Mer	https://securityaffairs.com/180780/cyber-crime/hacking-group-d4rk4rmy-claimed-the-hack-of-monte-carlo-societe-des-bains-de-mer.html
$1 Million Offered for WhatsApp Exploit at Pwn2Own Ireland 2025	https://www.securityweek.com/1-million-offered-for-whatsapp-exploit-at-pwn2own-ireland-2025/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Vietnamese Hackers Use PXA Stealer, Hit 4,000 IPs and Steal 200,000 Passwords Globally	https://thehackernews.com/2025/08/vietnamese-hackers-use-pxa-stealer-hit.html
Northwest Radiologists data breach hits 350,000 in Washington	https://securityaffairs.com/180772/data-breach/northwest-radiologists-data-breach-hits-350000-in-washington.html
Ransomware Attack on Phone Repair and Insurance Company Cause Millions in Damage	https://cybersecuritynews.com/ransomware-attack-on-phone-repair/
New Python-Based PXA Stealer Via Telegram Stolen 200,000 Unique Passwords and Hundreds of Credit Cards	https://cybersecuritynews.com/pxa-stealer-via-telegram-stolen-200000-unique-passwords/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
SonicWall Investigating Potential SSL VPN Zero-Day After 20+ Targeted Attacks Reported	https://thehackernews.com/2025/08/sonicwall-investigating-potential-ssl.html
Researchers Exploited Google kernelCTF Instances And Debian 12 With A 0-Day	https://cybersecuritynews.com/exploit-google-kernelctf-instances/
CL-STA-0969 Installs Covert Malware in Telecom Networks During 10-Month Espionage Campaign	https://thehackernews.com/2025/08/cl-sta-0969-installs-covert-malware-in.html
WAFs protection Bypassed to Execute XSS Payloads Using JS Injection with Parameter Pollution	https://cybersecuritynews.com/wafs-protection-bypassed/
Raspberry Robin Malware Downloader Attacking Windows Systems With New Exploit for Common Log File System Driver Vulnerability	https://cybersecuritynews.com/raspberry-robin-malware-downloader/

Claude Vulnerabilities Let Attackers Execute Unauthorized Commands With its Own Help	https://cybersecuritynews.com/claude-vulnerabilities/
FUJIFILM Printers Vulnerability Let Attackers Trigger DoS Condition	https://cybersecuritynews.com/fujifilm-printers-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Several Vulnerabilities Patched in AI Code Editor Cursor	https://www.securityweek.com/several-vulnerabilities-patched-in-ai-code-editor-cursor/
Nvidia Patches Critical RCE Vulnerability Chain	https://www.darkreading.com/vulnerabilities-threats/nvidia-patches-critical-rce-vulnerability-chain

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Ransomware gangs join attacks targeting Microsoft SharePoint servers	https://www.bleepingcomputer.com/news/security/ransomware-gangs-join-attacks-targeting-microsoft-sharepoint-servers/
New LegalPwn Attack Exploits Gemini, ChatGPT and other AI Tools into Executing Malicious Code via Disclaimers	https://cybersecuritynews.com/legalpwn-attack/
New Plague Linux malware stealthily maintains SSH access	https://www.bleepingcomputer.com/news/security/new-plague-malware-backdoors-linux-devices-removes-ssh-session-traces/
APT37 Hackers Weaponizes JPEG Files to Attack Windows Systems Leveraging "mspaint.exe"	https://cybersecuritynews.com/apt37-hackers-weaponizes-jpeg-files/
NVIDIA Triton Bugs Let Unauthenticated Attackers Execute Code and Hijack AI Servers	https://thehackernews.com/2025/08/nvidia-triton-bugs-let-unauthenticated.html
New Android Malware Mimics as SBI Card, Axis Bank Apps to Steal Users Financial Data	https://cybersecuritynews.com/new-android-malware-mimics-as-sbi-card/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/
10 Best Vulnerability Management Tools In 2025	https://cybersecuritynews.com/vulnerability-management-tools/

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.

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/