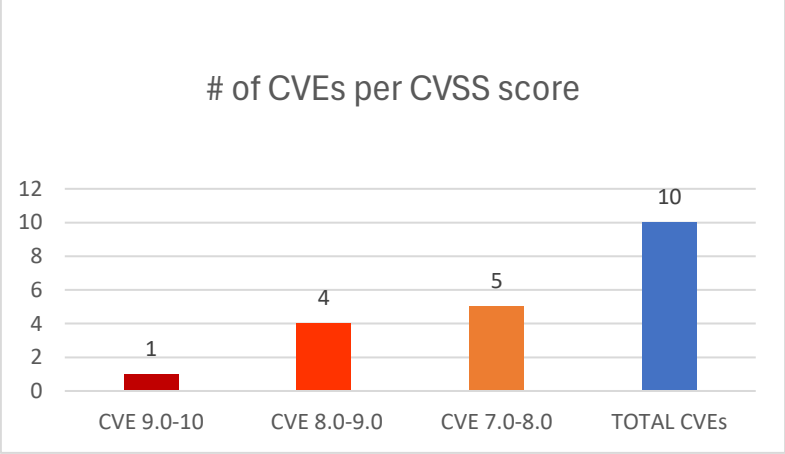
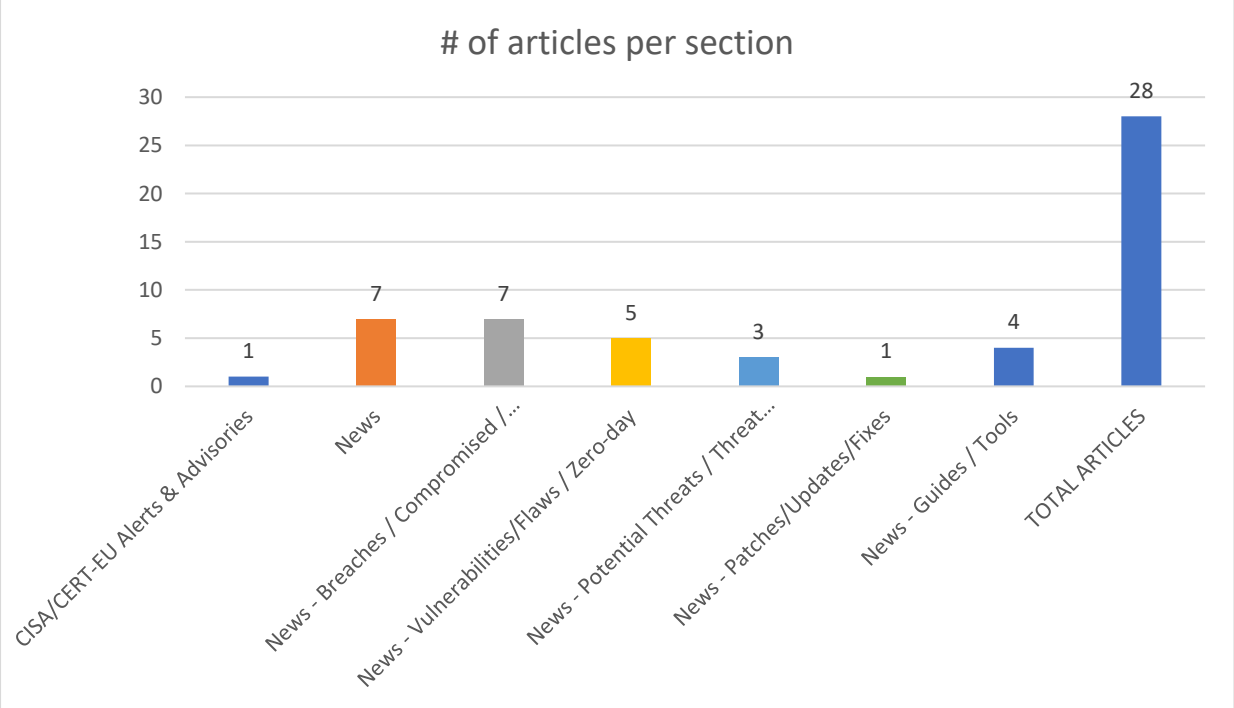
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 23/08/2025 - 26/08/2025





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-2025-7642	9,8	The Simpler Checkout plugin for WordPress	Authentication Bypass Using an Alternate Path or Channel	in versions 0.7.0 to 1.1.9	https://plugins.trac.wordpress.org/browser/simpler-checkout/tags/1.1.9/includes/hooks.php#L7 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/02cf0e1a-bd12-44b1-9bc5-1a5ec332b000?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9443	8,8	Tenda CH22	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1.0.0.1	https://github.com/moweizhang1994/cve/issues/4 VulDB https://vuldb.com/?ctiid.321281 VulDB https://vuldb.com/?id.321281 VulDB https://vuldb.com/?submit.634271 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-9379	8,6	Belkin	Insufficient Verification of Data Authenticity	AX1800 1.1.00.016	https://github.com/IOTRes/IOT_Firmware_Update/blob/main/Belkin/AX1800.md VulDB https://vuldb.com/?ctiid.321212 VulDB https://vuldb.com/?id.321212 VulDB https://vuldb.com/?submit.628641
https://nvd.nist.gov/vuln/detail/CVE-2025-9380	8,5	FNKvision Y215 CCTV Camera	Use of Hard-coded Password	10.194.120.40	https://vorachat.somsuay.com/blog/Hacking%20CCTV%20FNKvision%20-%20Y215 VulDB https://vorachat.somsuay.com/blog/Hacking%20CCTV%20FNKvision%20-%20Y215/#vulnerability-1-hard-coded-root-credentials-in-multiple-binaries VulDB https://vuldb.com/?ctiid.321213 VulDB https://vuldb.com/?id.321213 VulDB https://vuldb.com/?submit.629810
https://nvd.nist.gov/vuln/detail/CVE-2025-9048	8,1	The Wptobe-memberships plugin for WordPress	External Control of File Name or Path	all versions up to, and including, 3.4.2	https://plugins.svn.wordpress.org/wptobe-memberships/trunk/bwlms-fields/bwlms-fields.php Wordfence https://plugins.trac.wordpress.org/browser/wptobe-memberships/trunk/bwlms-fields/bwlms-fields.php#L156 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/466568c5-33a9-4891-b4ad-9bc6052603cb?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-9357	7,4	Linksys	Stack-based Buffer Overflow	RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001	https://github.com/wudipjq/my_vuln/blob/main/Linksys/vuln_25/25.md VulDB https://github.com/wudipjq/my_vuln/blob/main/Linksys/vuln_25/25.md#poc VulDB https://vuldb.com/?ctiid.321060 VulDB https://vuldb.com/?id.321060 VulDB https://vuldb.com/?submit.631529 VulDB https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-9476	7,3	SourceCodester Human Resource Information System	Improper Access Control	1.0	https://github.com/lrjbsyh/CVE_Hunter/issues/5 VulDB https://github.com/lrjbsyh/CVE_Hunter/issues/5#issue-3322736605 VulDB https://vuldb.com/?ctiid.321345 VulDB https://vuldb.com/?id.321345 VulDB https://vuldb.com/?submit.634757 VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-9473	7,3	SourceCodester Online Bank Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/August829/Yu/blob/main/58ead8e7e08bfb0e2.md VulDB https://vuldb.com/?ctiid.321342 VulDB https://vuldb.com/?id.321342 VulDB https://vuldb.com/?submit.634362 VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-9444	7,3	1000projects Online Project Report Submission and Evaluation System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/yunhdeng/CVE/issues/1 VulDB https://vuldb.com/?ctiid.321282 VulDB https://vuldb.com/?id.321282 VulDB https://vuldb.com/?submit.634272
https://nvd.nist.gov/vuln/detail/CVE-2025-9426	7,3	Online Tour and Travel Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/shq3526/cve/issues/7 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.321269 VulDB https://vuldb.com/?id.321269 VulDB https://vuldb.com/?submit.634154

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2024-8069 Citrix Session Recording Deserialization of Untrusted Data Vulnerability ▪ CVE-2024-8068 Citrix Session Recording Improper Privilege Management Vulnerability ▪ CVE-2025-48384 Git Link Following Vulnerability	https://www.cisa.gov/news-events/alerts/2025/08/25/cisa-adds-three-known-exploited-vulnerabilities-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
MITRE Updates List of Most Common Hardware Weaknesses	https://www.securityweek.com/mitre-updates-list-of-most-common-hardware-weaknesses/
Chinese Developer Jailed for Deploying Malicious Code at US Company	https://www.infosecurity-magazine.com/news/chinese-developer-malicious-code-us/
CISA Seeks Biden Era's SBOM Minimum Requirements Guideline Change	https://www.infosecurity-magazine.com/news/cisa-seeks-sbom-requirements-change/
Chinese UNC6384 Hackers Leverages Valid Code Signing Certificates to Evade Detection	https://cybersecuritynews.com/chinese-unc6384-hackers/
Hackers Sabotage Iranian Ships Using Maritime Communications Terminals in Its MySQL Database	https://cybersecuritynews.com/hackers-sabotage-iranian-ships-using-maritime-communications/
NIST Publish 'Lightweight Cryptography' Standard To Protect IoT Devices	https://cybersecuritynews.com/nist-publish-lightweight-cryptography-standard/
CISA Warns of Citrix RCE and Privilege Escalation Vulnerabilities Exploited in Attacks	https://cybersecuritynews.com/cisa-warns-of-citrix-vulnerabilities/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
National Public Data Relaunches Despite 2.9 Billion SSNs Breach	https://hackread.com/national-public-data-relaunch-despite-ssns-breach/?&web_view=true
New Jersey social services org notifies 42K people of data breach that leaked SSNs, medical and financial info	https://www.comparitech.com/news/new-jersey-social-services-org-notifies-42k-people-of-data-breach-that-leaked-ssns-medical-and-financial-info/?&web_view=true
Farmers Insurance says 1 million customers affected by cyberattack on third-party vendor	https://therecord.media/farmers-insurance-million-data-breach?&web_view=true
Auchan retailer data breach impacts hundreds of thousands of customers	https://www.bleepingcomputer.com/news/security/auchan-retailer-data-breach-impacts-hundreds-of-thousands-of-customers/
Arch Linux Confirms Week-Long DDoS Attack Disrupted its Website, Repository, and Forums	https://cybersecuritynews.com/arch-linux-ddos-attack/
KorPlug Malware Unmasked – TTPs, Control Flow, IOCs Exposed	https://cybersecuritynews.com/korplug-malware-unmasked/

Hundreds of Thousands of Users' Grok Chats Exposed in Google Search Results	https://cybersecuritynews.com/grok-chats-exposed-in-google-search-results/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
0-Click Zendesk Account Takeover Vulnerability Enables Access to all Zendesk Tickets	**https://cybersecuritynews.com/zendesk-account-takeover-vulnerability/**
New Stealthy Malware Exploiting Cisco, TP-Link and Other Routers to Gain Remote Control	**https://cybersecuritynews.com/new-stealthy-malware-exploiting-cisco-tp-link/**
Multiple vtenext Vulnerabilities Let Attackers Bypass Authentication and Execute Remote Codes	https://cybersecuritynews.com/vtenext-vulnerabilities/
Critical Tableau Server Vulnerability Let Attackers Upload Malicious Files	https://cybersecuritynews.com/tableau-server-vulnerability/
PoC Exploit & Vulnerability Analysis Released for Apple 0-Day RCE Vulnerability	https://cybersecuritynews.com/apple-0-day-rce-poc-exploit/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Docker Fixes CVE-2025-9074, Critical Container Escape Vulnerability With CVSS Score 9.3	**https://thehackernews.com/2025/08/docker-fixes-cve-2025-9074-critical.html**

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Password Managers Vulnerable to Data Theft via Clickjacking	**https://www.securityweek.com/password-managers-vulnerable-to-data-theft-via-clickjacking/**
Hackers Can Exfiltrate Windows Secrets and Credentials Silently by Evading EDR Detection	**https://cybersecuritynews.com/exfiltrate-windows-secrets-and-credentials/**
Hackers Actively Scanning to Exploit Microsoft Remote Desktop Protocol Services From 30,000+ IPs	https://cybersecuritynews.com/microsoft-remote-desktop-protocol-services/

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/
Top 15 Best Security Incident Response Tools In 2025	https://cybersecuritynews.com/incident-response-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-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/