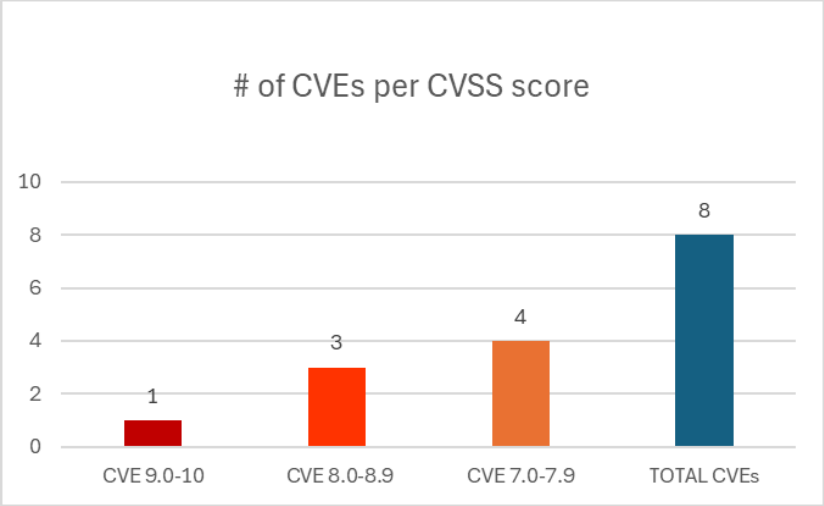
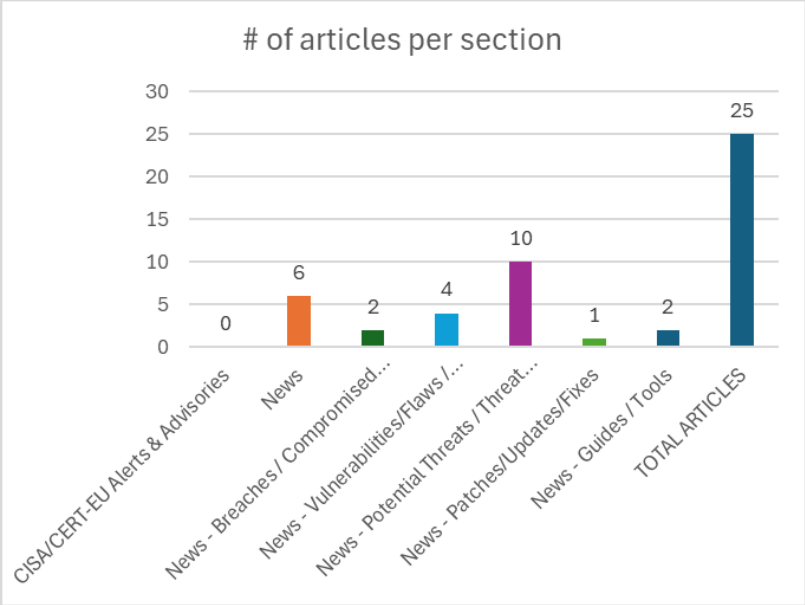
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 23/05/2025 - 27/05/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv 3	Προϊόν/ Υπηρε-σία	Τύπος Ευπά-θειας	Συ-σκευές/Εκδόσεις που επη-ρεάζο-νται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-5058	**9,8**	The eMagi-cOne Store Manager for Woo-Com-merce plugin for Word-Press	Unre-stricted Upload of File with Danger-ous Type	all ver-sions up to, and including, 1.2.5	https://github.com/d0n601/CVE-2025-5058/ https://plugins.trac.wordpress.org/browser/store-manager-connector/trunk/classes/class-emosmconnectorcommon.php#L2115 https://plugins.trac.wordpress.org/browser/store-manager-connector/trunk/classes/class-emosmcwoocommerceover-rider.php#L272 https://ryankozak.com/posts/cve-2025-5058/ https://www.wordfence.com/threat-intel/vulnerabilities/id/8a00ece0-6644-4535-86aa-d0802d94a1a7?source=cve
https://nvd.nist.gov/vuln/de-tail/CVE-2025-5126	**8,8**	FLIR	Improper Neutrali-zation of Special Elements used in a Com-mand ('Com-mand In-jection')	AX8 up to 1.46.16	https://github.com/YZS17/CVE/blob/main/Remote%20Command%20Injection%20in%20parameter%20%24hour.md https://github.com/YZS17/CVE/blob/main/Remote%20Command%20Injection%20in%20parameter%20%24minute.md https://vuldb.com/?ctiid.310204 https://vuldb.com/?id.310204 https://vuldb.com/?submit.570725
https://nvd.nist.gov/vuln/detail/CVE-2025-5156	**8,8**	H3C	Buffer Copy without Checking Size of In-put ('Classic Buffer Over-flow')	GR-5400AX up to 100R008	https://github.com/CH13hh/tmp_store_cc/blob/main/H3C%20GB5400AX/6.md https://vuldb.com/?ctiid.310244 https://vuldb.com/?id.310244 https://vuldb.com/?submit.574080

https://nvd.nist.gov/vuln/detail/CVE-2025-5124	**8,1**	Sony	Use of Default Credentials	SNC-M1, SNC-M3, SNC-RZ25N, SNC-RZ30N, SNC-DS10, SNC-CS3N and SNC-RX570N up to 1.30	https://github.com/zeke2997/CVE_request_Sony https://github.com/zeke2997/CVE_request_Sony#3-poc https://vuldb.com/?ctiid.310203 https://vuldb.com/?id.310203 https://vuldb.com/?submit.564839
https://nvd.nist.gov/vuln/detail/CVE-2025-5119	**7,3**	Emlog	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Pro 2.5.11	https://github.com/404heihei/CVE/issues/5 https://github.com/404heihei/CVE/issues/5 https://vuldb.com/?ctiid.310198 https://vuldb.com/?id.310198 https://vuldb.com/?submit.555822
https://nvd.nist.gov/vuln/detail/CVE-2025-5128	**7,3**	ScriptAndTools Real-Estate-website-in-PHP	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://vuldb.com/?ctiid.310206 https://vuldb.com/?id.310206 https://vuldb.com/?submit.570957 https://www.websecurityinsights.my.id/2025/05/script-and-tools-real-estate-management.html

https://nvd.nist.gov/vuln/detail/CVE-2025-5139	**7,3**	Qualitor	Improper Neutralization of Special Elements used in a Command ('Command Injection')	8.20	https://gist.githubusercontent.com/MatheuZSecurity/fe221fd5b2e5393abf76be42f11f52c3/raw/e8d9c63885f0b83b3374db3d31dbe2c69c868334/poc.sh https://vuldb.com/?ctiid.310220 https://vuldb.com/?id.310220 https://vuldb.com/?submit.572477 https://www.youtube.com/watch?v=Dq4C5s9Uwyo
https://nvd.nist.gov/vuln/detail/CVE-2025-5129	**7,0**	Sangfor	Untrusted Search Path	2.3.10.60	https://drive.google.com/file/d/1_zGvKXIFLdh5RtxauvNYSa52YONJmY9q/view https://vuldb.com/?ctiid.310207 https://vuldb.com/?id.310207 https://vuldb.com/?submit.571267 https://www.notion.so/Sangfor-Zero-Trust-Access-Control-System-ATrust-Privilege-Escalation-Vulnerability-1eab06dd544b802b87cdd6ba6b70cce9

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL

News

Σύντομη περιγραφή / Τίτλος	URL
Fake software activation videos on TikTok spread Vidar, StealC	https://securityaffairs.com/178269/cyber-crime/fake-software-activation-videos-on-tiktok-spread-vidar-stealc.html
NIST Introduces New Metric to Measure Likelihood of Vulnerability Exploits	https://www.infosecurity-magazine.com/news/nist-metric-lev-likelihood/
ChatGPT Deep Research can now pull data from Dropbox and Box	https://www.bleepingcomputer.com/news/artificial-intelligence/chatgpt-deep-research-can-now-pull-data-from-drop-box-and-box/
Operation ENDGAME disrupted global ransomware infrastructure	https://securityaffairs.com/178245/cyber-crime/operation-endgame-disrupted-global-ransomware-infrastructure.html
Nova Scotia Power Confirms Ransomware Attack – 280k Customers Affected	https://cybersecuritynews.com/nova-scotia-ransomware-attack/
ChatGPT o3 Model Bypassed to Sabotage the Shutdown Mechanism	https://cybersecuritynews.com/chatgpt-o3-model-bypassed/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
iOS Sleep App Exposes Personal and Health Data of Over 25,000 Users	https://dailysecurityreview.com/security-spotlight/ios-sleep-app-exposes-personal-and-health-data-of-over-25000-users/
184 Million Users' Passwords Exposed From an Open Directory Controlled by Hackers	https://cybersecuritynews.com/184-million-users-passwords-exposed/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
O2 VoLTE Vulnerability Exposes Location of Any Customer With a Phone Call	https://cybersecuritynews.com/o2-volte-vulnerability-exposes-location/
Multiple pfSense Firewall Vulnerabilities Let Attackers Inject Malicious Codes	https://cybersecuritynews.com/pfsense-firewall-vulnerabilities/
Oracle TNS Protocol Vulnerability Let Attackers Access System Memory Contents	https://cybersecuritynews.com/oracle-tns-protocol-vulnerability/
Multiple GitLab Vulnerabilities Let Attackers Trigger DoS Attacks	https://cybersecuritynews.com/multiple-gitlab-vulnerabilities/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Linux 6.15 Released with Several New Features & Improvements	https://cybersecuritynews.com/linux-6-15-released/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Week in review: Trojanized KeePass allows ransomware attacks, cyber risks of AI hallucinations	https://www.helpnetsecurity.com/2025/05/25/week-in-review-trojanized-keepass-allows-ransomware-attacks-cyber-risks-of-ai-hallucinations/
Hackers Use Fake VPN and Browser NSIS Installers to Deliver Winos 4.0 Malware	https://thehackernews.com/2025/05/hackers-use-fake-vpn-and-browser-nsis.html
Vulnerability in Popular macOS App Cursor Allows Malware to Bypass Privacy Protections, Exposing User Data	https://cybersecuritynews.com/vulnerability-in-popular-macos-app-cursor/
Hard-Coded Telnet Credentials Leave D-Link Routers Wide Open to Remote Code Execution	https://cybersecuritynews.com/hard-coded-telnet-credentials-d-link-routers/
FBI Warns of Silent Ransom Group Attacking Users Via Fake IT Calls	https://cybersecuritynews.com/fbi-warns-of-silent-ransom-group/
Katz Stealer Attacking Chrome, Edge, Brave & Firefox to Steal Login Details	https://cybersecuritynews.com/katz-stealer-attacking-chrome-edge-brave-firefox/
Street-Level QR Phishing: Cybercriminals Take Social Engineering to the Real World	https://cybersecuritynews.com/street-level-qr-phishing/
Apache Tomcat Vulnerability Allows Remote Code Execution – PoC Released	https://cybersecuritynews.com/apache-tomcat-vulnerability-poc-released/
Oracle TNS Protocol Vulnerability Let Attackers Access System Memory Contents	https://cybersecuritynews.com/oracle-tns-protocol-vulnerability/
40+ Malicious Chrome Extensions Mimic as Popular Chrome Brands Steals Sensitive Data	https://cybersecuritynews.com/malicious-chrome-extensions-mimic-as-popular-chrome-brands/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
10 Best NGINX Monitoring Tools – 2025	https://cybersecuritynews.com/best-nginx-monitoring-tools/
Hands-on Malware Analysis Training to Boost Up SOC & MSSP Teams	https://cybersecuritynews.com/malware-analysis-training/

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/