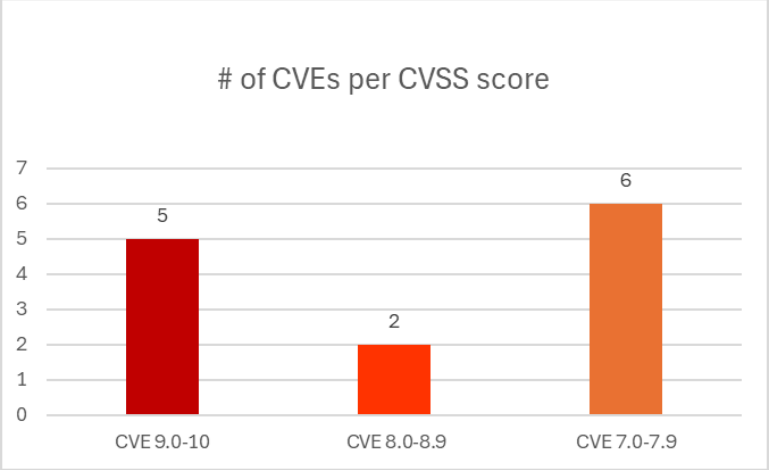
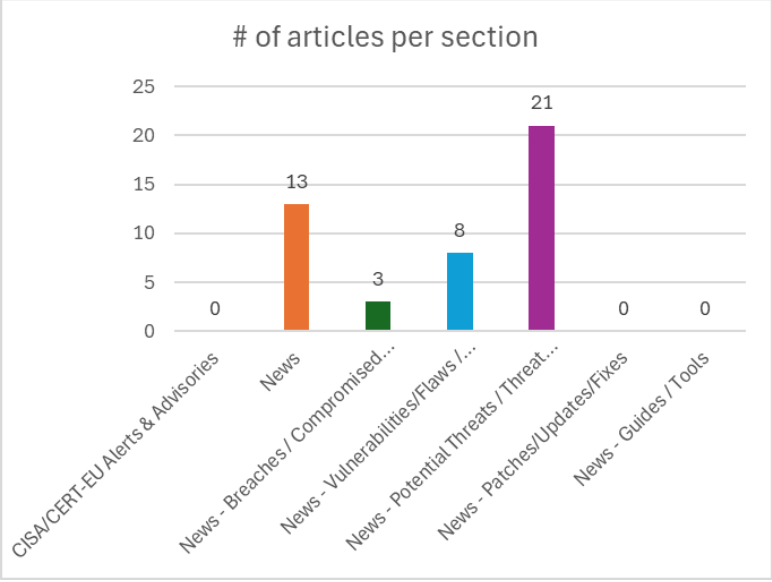
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 05/09/2025 - 09/09/2025





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-2025-54914	10.0	Azure	Improper Access Control	Azure Networking Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-54914
https://nvd.nist.gov/vuln/detail/CVE-2025-55190	9.9	Argo CD	Exposure of Sensitive Information to an Unauthorized Actor	versions 2.13.0 through 2.13.8, 2.14.0 through 2.14.15, 3.0.0 through 3.0.12 and 3.1.0-rc1 through 3.1.1	https://github.com/argoproj/argo-cd/commit/e8f86101f5378662ae6151ce5c3a76e9141900e8 https://github.com/argoproj/argo-cd/security/advisories/GHSA-786q-9hcg-v9ff
https://nvd.nist.gov/vuln/detail/CVE-2025-55037	9.3	TkEasyGUI	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	TkEasyGUI versions prior to v1.0.22	https://github.com/kujirahand/tkeasygui-python/releases/tag/v1.0.22 https://jvn.jp/en/jp/JVN48739895/
https://nvd.nist.gov/vuln/detail/CVE-2025-55241	9.0	Azure	Improper Authentication	Azure Entra Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55241
https://nvd.nist.gov/vuln/detail/CVE-2025-55244	9.0	Azure	Improper Access Control	Azure Bot Service Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55244
https://nvd.nist.gov/vuln/detail/CVE-2025-58437	8.1	Coder	Insecure Inherited Permissions	Versions 2.22.0 through 2.24.3, 2.25.0 and 2.25.1	https://github.com/coder/coder/commit/06cbb2890f453cd522bb2158a6549afa3419c276 https://github.com/coder/coder/commit/20d67d7d7191a4fd5d36a61c6fc1e23ab59befc0 https://github.com/coder/coder/commit/ec660907faa0b0eae20fa2ba58ce1733f5f4b35a https://github.com/coder/coder/pull/19667 https://github.com/coder/coder/pull/19668 https://github.com/coder/coder/pull/19669 https://github.com/coder/coder/security/advisories/GHSA-j6xf-jwrj-v5qp
https://nvd.nist.gov/vuln/detail/CVE-2025-58439	8.1	ERP	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Versions below 14.89.2 and 15.0.0 through 15.75.1	https://github.com/frappe/erpnext/pull/49219 https://github.com/frappe/erpnext/pull/49220 https://github.com/frappe/erpnext/security/advisories/GHSA-fvjw-5w9q-6v39
https://nvd.nist.gov/vuln/detail/CVE-2021-26383	7.9	AMD TEE (Trusted Execution Environment)	Out-of-bounds Write		https://www.amd.com/en/resources/product-security/bulletin/AMD-SB-4012.html https://www.amd.com/en/resources/product-security/bulletin/AMD-SB-5007.html https://www.amd.com/en/resources/product-security/bulletin/AMD-SB-6018.html

https://nvd.nist.gov/vuln/detail/CVE-2025-32320	**7.8**	Android	Unintended Proxy or Intermediary ('Confused Deputy')		https://source.android.com/security/bulletin/android-16
https://nvd.nist.gov/vuln/detail/CVE-2025-58374	**7.8**	Roo Code	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Versions 3.25.23 and below	https://github.com/RooCodeInc/Roo-Code/pull/7390/files https://github.com/RooCodeInc/Roo-Code/releases/tag/v3.26.0 https://github.com/RooCodeInc/Roo-Code/security/advisories/GHSA-c292-qxq4-4p2v
https://nvd.nist.gov/vuln/detail/CVE-2025-58362	**7.5**	Hono	Use of Incorrectly-Resolved Name or Reference	Versions 4.8.0 through 4.9.5	https://github.com/honojs/hono/commit/1d79aedc3f82d8c9969b115fe61bc4bd705ec8de https://github.com/honojs/hono/releases/tag/v4.9.6 https://github.com/honojs/hono/security/advisories/GHSA-9hp6-4448-45g2
https://nvd.nist.gov/vuln/detail/CVE-2025-58780	**7.2**	ScienceLogic	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	ScienceLogic SL1 before 12.1.1	https://docs.sciencelogic.com/release_notes_html/Content/12-1-1/12-1-1_release_notes.htm#New_Features_in_12-1-1 https://github.com/SexyShoelessGodofWar/CVE-2025-58780
https://nvd.nist.gov/vuln/detail/CVE-2025-48104	**7.1**	Window Music Player	Cross-Site Request Forgery (CSRF)	from n/a through 3.4.2	https://patchstack.com/database/wordpress/plugin/floating-window-music-player/vulnerability/wordpress-floating-window-music-player-plugin-3-4-2-cross-site-request-forgery-csrf-to-stored-xss-vulnerability?_s_id=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL

News

Σύντομη περιγραφή / Τίτλος	URL
Weekly Cybersecurity News Recap : Palo Alto Networks, Zscaler, Jaguar Land Rover, and Cyber Attacks	https://cybersecuritynews.com/weekly-cybersecurity-news-sept/
Top 10 Best Cloud Penetration Testing Companies in 2025	https://cybersecuritynews.com/best-cloud-penetration-testing-companies/
Kali Linux vs Parrot OS – Which Penetration Testing Platform is Most Suitable for Cybersecurity Professionals?	https://cybersecuritynews.com/kali-linux-vs-parrot-os/
10 Best Internal Network Penetration Testing Companies in 2025	https://cybersecuritynews.com/internal-network-penetration-testing-companies/
Hackers Use AI Platforms to Steal Microsoft 365 Credentials in Phishing Campaign	https://cybersecuritynews.com/ai-platforms-leveraged-microsoft-365/
Hackers Leverage Raw Disk Reads to Bypass EDR Solutions and Access Highly Sensitive Files	https://cybersecuritynews.com/edr-bypass-via-disk-reads/
CISA Warns of Linux Kernel Race Condition Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-linux-kernel-race-condition-vulnerability/
Windows Heap-based Buffer Overflow Vulnerability Let Attackers Elevate Privileges	https://cybersecuritynews.com/windows-heap-based-buffer-overflow-vulnerability/
Hackers Hijacked 18 Very Popular npm Packages With 2 Billion Weekly Downloads	https://cybersecuritynews.com/npm-packages-hijacked/
Progress OpenEdge AdminServer Vulnerability Let Attackers Execute Remote Code	https://cybersecuritynews.com/progress-openedge-adminserver-vulnerability/
Windows Defender Vulnerability Allows Service Hijacking and Disablement via Symbolic Link Attack	https://cybersecuritynews.com/windows-defender-vulnerability/
Microsoft Azure Cloud Disrupted by Undersea Cable Cuts in Red Sea	https://cybersecuritynews.com/microsoft-azure-undersea-cable/
How Microsoft Azure Storage Logs Aid Forensics Following a Security Breach	https://cybersecuritynews.com/microsoft-azure-storage-forensics/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Wealthsimple Data Breach Exposes Personal Information of Some Users	https://cybersecuritynews.com/wealthsimple-data-breach/
Qualys Confirms Data Breach – Hackers Accessed Salesforce Data in Supply Chain Attack	https://cybersecuritynews.com/qualys-confirms-data-breach/
Tenable Confirms Data Breach – Hackers Accessed Customers' Contact Details	https://cybersecuritynews.com/tenable-confirms-data-breach/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Critical Argo CD API Vulnerability Exposes Repository Credentials	https://cybersecuritynews.com/argo-cd-api-vulnerability/
Critical SAP S/4HANA Vulnerability Actively Exploited to Fully Compromise Your SAP System	https://cybersecuritynews.com/sap-s-4hana-vulnerability-actively-exploited/
CISA Warns of Android 0-Day Use-After-Free Vulnerability Exploited in Attacks	https://cybersecuritynews.com/android-0-day-use-after-free-vulnerability/
Critical 0-Click Vulnerability Enables Attackers to Takeover Email Access Using Punycode	https://cybersecuritynews.com/0-click-email-vulnerability/
Hackers Scanning Cisco ASA Devices to Exploit Vulnerabilities from 25,000 Ips	https://cybersecuritynews.com/hackers-scanning-cisco-asa-devices-to-exploit-vulnerabilities-from-25000-ips/
PgAdmin Vulnerability Lets Attackers Gain Unauthorised Account Access	https://cybersecuritynews.com/pgadmin-vulnerability/
PoC Exploit Released for ImageMagick RCE Vulnerability – Update Now	https://cybersecuritynews.com/poc-imagemagick-rce-vulnerability/
Apache Jackrabbit Exposes Systems To Arbitrary Code Execution Attacks	https://cybersecuritynews.com/apache-jackrabbit-exposes-systems/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
“GPUGate” Malware Abuses Google Ads and GitHub to Deliver Advanced Malware Payload	https://cybersecuritynews.com/gpugate-abuses-google-ads/
New Report Claims Microsoft Used China-Based Engineers For SharePoint Support and Bug Fixing	https://cybersecuritynews.com/new-report-claims-microsoft-used-china-based-engineers/
143,000 Malware Files Attacked Android and iOS Device Users in Q2 2025	https://cybersecuritynews.com/143000-malware-files-attacked-android/
SafePay Ransomware Claiming Attacks Over 73 Victim Organizations in a Single Month	https://cybersecuritynews.com/safepay-ransomware-claiming-attacks-over-73-victim/
TAG-150 Hackers Deploying Self-Developed Malware Families to Attack Organizations	https://cybersecuritynews.com/tag-150-hackers-deploying-self-developed-malware/
Threats Actors Weaponize ScreenConnect Installers to Gain Initial Access to Organizations	https://cybersecuritynews.com/threats-actors-weaponize-screenconnect-installers/
New Malware Leverages Windows Character Map to Bypass Windows Defender and Mine Cryptocurrency for The Attackers	https://cybersecuritynews.com/new-malware-leverages-windows-character-map/
Hackers Weaponize Fake Microsoft Teams Site to Deploy Odyssey macOS Stealer	https://cybersecuritynews.com/fake-microsoft-teams-site-weaponized/
North Korean Threat Actors Reveal Their Tactics in Replacing Infrastructure With New Assets	https://cybersecuritynews.com/north-korean-threat-actors-reveal-their-tactics/
Hackers Leverages Google Calendar APIs With Serverless MeetC2 Communication Framework	https://cybersecuritynews.com/hackers-leverages-google-calendar-apis/
New NightshadeC2 Botnet Uses ‘UAC Prompt Bombing’ to Bypass Windows Defender Protections	https://cybersecuritynews.com/new-nightshadec2-botnet-uses-uac-prompt-bombing/
Colombian Malware Weaponizing SWF and SVG to Bypass Detection	https://cybersecuritynews.com/colombian-malware-weaponizing-swf-and-svg/
Venezuela’s Maduro Says Huawei Mate X6 Gift From China is Unhackable by U.S. Spies	https://cybersecuritynews.com/venezuelas-maduro-says-huawei-mate-x6/
LunaLock Ransomware Attacking Artists to Steal and Encrypt Data	https://cybersecuritynews.com/lunalock-ransomware-attacking-artists/
Exposed ‘Kim’ Dump Exposes Kimsuky Hackers New Tactics, Techniques, and Infrastructure	https://cybersecuritynews.com/exposed-kim-dump-exposes-kimsuky-hackers/
Hackers Weaponize Amazon Simple Email Service to Send 50,000+ Malicious Emails Per Day	https://cybersecuritynews.com/hackers-weaponizee-amazon-simple-email-service/
Researchers Bypassed Web Application Firewall With JS Injection with Parameter Pollution	https://cybersecuritynews.com/researchers-bypassed-web-application-firewall/
U.S. Authorities Investigating Malicious Email Targeting Trade Talks with China	https://cybersecuritynews.com/u-s-authorities-investigating-malicious-email/
Atomic Stealer Disguised as Cracked Software Attacking macOS Users	https://cybersecuritynews.com/atomic-stealer-disguised-as-cracked-software/
Australian Authorities Uncovered Activities and Careers of Ransomware Criminal Groups	https://cybersecuritynews.com/australian-authorities-uncovered-activities/
Lazarus APT Hackers Using ClickFix Technique to Steal Sensitive Intelligence Data	https://cybersecuritynews.com/lazarus-apt-hackers-using-clickfix-technique/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL

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/