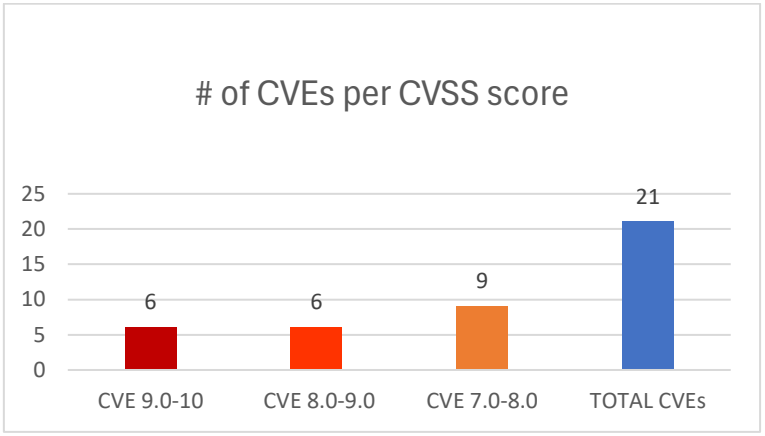
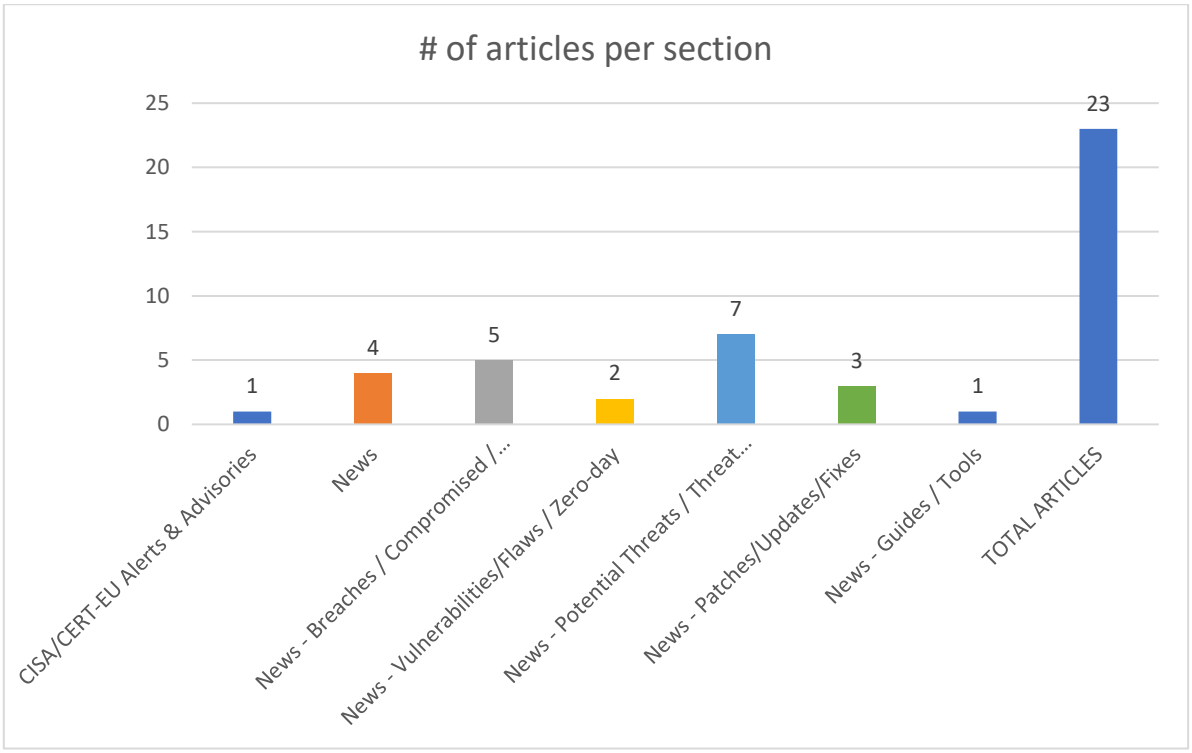
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/06/2025 - 20/06/2025





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-2025-49217	9,8	Trend Micro Endpoint Encryption PolicyServer	Use of Obsolete Function		https://success.trendmicro.com/en-US/solution/KA-0019928 https://www.zerodayinitiative.com/advisories/ZDI-25-374/
https://nvd.nist.gov/vuln/detail/CVE-2025-50201	9,8	WeGIA	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to version 3.4.2	https://github.com/LabRedesCefetRJ/WeGIA/commit/45f32ad1d52775fc99f3c90075c8136c6d4d1d3d https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-52p5-5fmw-9hrf
https://nvd.nist.gov/vuln/detail/CVE-2025-24288	9,8	The Versa Director software			https://security-portal.versa-networks.com/emailbulletins/68526d12dc94d6b9f2faf719 https://support.versa-networks.com/support/solutions/articles/23000026708-release-22-1-4
https://nvd.nist.gov/vuln/detail/CVE-2025-26199	9,8	CloudClassroom PHP Project	Cleartext Transmission of Sensitive Information	v.1.0	https://gist.github.com/tansique-17/6e01bb1b8a09ef499a9b8484a8dc2487
https://nvd.nist.gov/vuln/detail/CVE-2025-20260	9,8	PDF scanning processes of ClamAV	Heap-based Buffer Overflow		https://blog.clamav.net/2025/06/clamav-143-and-109-security-patch.html
https://nvd.nist.gov/vuln/detail/CVE-2025-52467	9,1	pgai	Exposure of Sensitive Information to an Unauthorized Actor	Prior to commit 8eb3567	https://github.com/timescale/pgai/commit/8eb356729c33560ce54b88b9a956960ad1e3ede8 https://github.com/timescale/pgai/pull/742 https://github.com/timescale/pgai/security/advisories/GHSA-89qq-hgvp-x37m

https://nvd.nist.gov/vuln/detail/CVE-2025-49215	8,8	Trend Micro Endpoint Encryption PolicyServer	Use of Inherently Dangerous Function		https://success.trendmicro.com/en-US/solution/KA-0019928 https://www.zerodayinitiative.com/advisories/ZDI-25-372/
https://nvd.nist.gov/vuln/detail/CVE-2025-6192	8,8	Metrics in Google Chrome	Use After Free	prior to 137.0.7151.119	https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_17.html https://issues.chromium.org/issues/421471016
https://nvd.nist.gov/vuln/detail/CVE-2025-5071	8,8	The AI Engine plugin for WordPress	Incorrect Authorization	versions 2.8.0 to 2.8.3	https://plugins.trac.wordpress.org/browser/ai-engine/tags/2.8.1/labs/mcp.php#L43 https://plugins.trac.wordpress.org/changeset/3313554/ai-engine#file21 https://www.wordfence.com/threat-intel/vulnerabilities/id/0e7654a1-0020-4bf1-86be-bdb238a9fe0d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-36049	8,8	IBM webMethods Integration Server	Improper Restriction of XML External Entity Reference	10.5, 10.7, 10.11, and 10.15	https://www.ibm.com/support/pages/node/7237146
https://nvd.nist.gov/vuln/detail/CVE-2025-6302	8,8	TOTOLINK	Stack-based Buffer Overflow	EX1200T 4.1.2cu.5232_B20210713	https://kn0sinna.notion.site/TOTOLINK-EX1200T-stack-based-BufferOverflow-vulnerability-20fb1876cd6e80d5b4d1f7ec16de4ec2 https://vuldb.com/?ctiid.313302 https://vuldb.com/?id.313302 https://vuldb.com/?submit.595473 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-20271	8,6	Cisco AnyConnect VPN server	Use of Uninitialized Variable	Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-sM5GCfm7

https://nvd.nist.gov/vuln/detail/CVE-2025-30640	7,8	Trend Micro Deep Security	Improper Link Resolution Before File Access ('Link Following')	20.0	https://success.trendmicro.com/en-US/solution/KA-0019344 https://www.zerodayinitiative.com/advisories/ZDI-25-239/
https://nvd.nist.gov/vuln/detail/CVE-2025-32412	7,8	Fuji Electric Smart Editor	Out-of-bounds Read		https://www.cisa.gov/news-events/ics-advisories/icsa-25-168-04
https://nvd.nist.gov/vuln/detail/CVE-2025-49385	7,8	Trend Micro Security	Windows Shortcut Following (.LNK)	17.8	https://helpcenter.trendmicro.com/en-us/article/TMKA-18461 https://www.zerodayinitiative.com/advisories/ZDI-25-380/
https://nvd.nist.gov/vuln/detail/CVE-2025-49211	7,7	Trend Micro Endpoint Encryption PolicyServer	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://success.trendmicro.com/en-US/solution/KA-0019928 https://www.zerodayinitiative.com/advisories/ZDI-25-368/
https://nvd.nist.gov/vuln/detail/CVE-2025-49715	7,5	Dynamics 365 FastTrack Implementation Assets	Exposure of Private Personal Information to an Unauthorized Actor		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49715
https://nvd.nist.gov/vuln/detail/CVE-2025-6296	7,3	Hostel Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/y2xsec324/cve/issues/1 https://vuldb.com/?ctiid.313298 https://vuldb.com/?id.313298 https://vuldb.com/?submit.594016]
https://nvd.nist.gov/vuln/detail/CVE-2025-6300	7,3	PHPGurukul Employee Record Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.3	https://github.com/GarminYoung/myCVE/issues/10 https://phpgurukul.com/ https://vuldb.com/?ctiid.313300 https://vuldb.com/?id.313300 https://vuldb.com/?submit.595366

https://nvd.nist.gov/vuln/detail/CVE-2025-6310	7,3	PHPGurukul Emergency Ambulance Hiring Portal	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/f1rstb100d/myCVE/issues/70 https://phpgurukul.com/ https://vuldb.com/?ctiid.313310 https://vuldb.com/?id.313310 https://vuldb.com/?submit.595917
https://nvd.nist.gov/vuln/detail/CVE-2025-6220	7,2	The Ultra Addons for Contact Form 7 plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 3.5.12	https://github.com/d0n601/CVE-2025-6220 https://plugins.trac.wordpress.org/browser/ultimate-addons-for-contact-form-7/trunk/admin/tf-options/classes/UACF7_Settings.php#L894-920 https://plugins.trac.wordpress.org/changeset/3288584/ https://ryankozak.com/posts/cve-2025-6220/ https://www.wordfence.com/threat-intel/vulnerabilities/id/697f3432-63b7-42d6-b188-812165cd2020?source=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
U.S. CISA adds Linux Kernel flaw to its Known Exploited Vulnerabilities catalog	▪ CVE-2023-0386 (CVSS score: 7.8)	https://securityaffairs.com/179104/hacking/u-s-cisa-adds-linux-kernel-flaw-to-its-known-exploited-vulnerabilities-catalog-2.html

News

Σύντομη περιγραφή / Τίτλος	URL
CISA warns of attackers exploiting Linux flaw with PoC exploit	https://www.bleepingcomputer.com/news/security/cisa-warns-of-attackers-exploiting-linux-flaw-with-poc-exploit/
Iranian bank purportedly breached by pro-Israel hacktivists	https://scmagazine.com/brief/iranian-bank-purportedly-breached-by-pro-israel-hacktivists
AI Now Generates Majority of Spam and Malicious Emails	https://www.infosecurity-magazine.com/news/ai-generates-spam-malicious-emails/
Ransomware Group Qilin Offers Legal Counsel to Affiliates	https://www.infosecurity-magazine.com/news/ransomware-qilin-offers-legal/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Healthcare services company Episource data breach impacts 5.4 Million people	https://securityaffairs.com/179115/data-breach/healthcare-services-company-episource-data-breach-impacts-5-4-million-people.html
New SuperCard Malware Using Hacked Android Phones to Relay Data from Users Payment Cards to Attackers Device	https://cybersecuritynews.com/new-supercard-malware-using-hacked-android-phones/
Telecom giant Viasat breached by China's Salt Typhoon hackers	https://www.bleepingcomputer.com/news/security/telecom-giant-viasat-breached-by-chinas-salt-typhoon-hackers/
UBS Employee Data Reportedly Exposed in Third Party Attack	https://www.infosecurity-magazine.com/news/ubs-employee-data-exposed-third/
Researchers discovered the largest data breach ever, exposing 16 billion login credentials	https://securityaffairs.com/179149/data-breach/researchers-discovered-the-largest-data-breach-ever-exposing-16-billion-login-credentials.html

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
New Linux Flaws Enable Full Root Access via PAM and Udisks Across Major Distributions	https://thehackernews.com/2025/06/new-linux-flaws-enable-full-root-access.html
Insecure GitHub Actions in Open Source Projects MITRE and Splunk Exposes Critical Vulnerabilities	https://cybersecuritynews.com/insecure-github-actions-in-open-source-projects-mitre/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Veeam Patches CVE-2025-23121: Critical RCE Bug Rated 9.9 CVSS in Backup & Replication	https://thehackernews.com/2025/06/veeam-patches-cve-2025-23121-critical.html
Critical Vulnerability Patched in Citrix NetScaler	https://www.securityweek.com/critical-vulnerability-patched-in-citrix-netscaler/
Chrome 137 Update Patches High-Severity Vulnerabilities	https://www.securityweek.com/chrome-137-update-patches-high-severity-vulnerabilities/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Famous Chollima Hackers Attacking Windows and MacOS Users With GolangGhost RAT	https://cybersecuritynews.com/famous-chollima-hackers-attacking-windows-and-macos-users/
1,500+ Minecraft Players Infected by Java Malware Masquerading as Game Mods on GitHub	https://thehackernews.com/2025/06/1500-minecraft-players-infected-by-java.html
Sitecore CMS exploit chain starts with hardcoded 'b' password	https://www.bleepingcomputer.com/news/security/sitecore-cms-exploit-chain-starts-with-hardcoded-b-password/
BlueNoroff Deepfake Zoom Scam Hits Crypto Employee with macOS Backdoor Malware	https://thehackernews.com/2025/06/bluenoroff-deepfake-zoom-scam-hits.html
200+ Trojanized GitHub Repositories Found in Campaign Targeting Gamers and Developers	https://thehackernews.com/2025/06/67-trojanized-github-repositories-found.html
GodFather Malware Upgraded to Hijack Legitimate Mobile Apps	https://www.infosecurity-magazine.com/news/godfather-upgraded-hijack-mobile/
AI hacking tools developed via commercial LLMs, report finds	https://scmagazine.com/brief/ai-hacking-tools-developed-via-commercial-llms-report-finds

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-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.

[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/