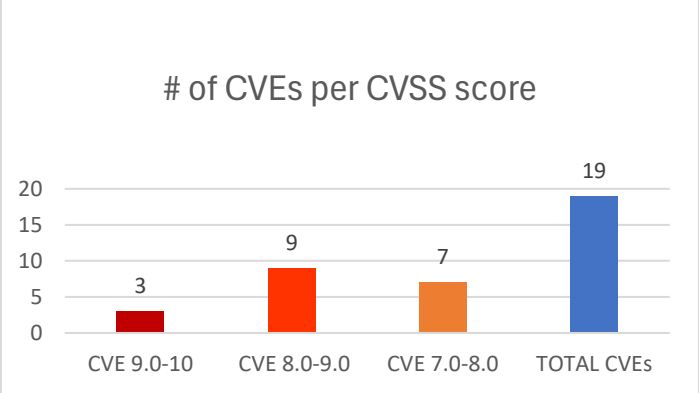
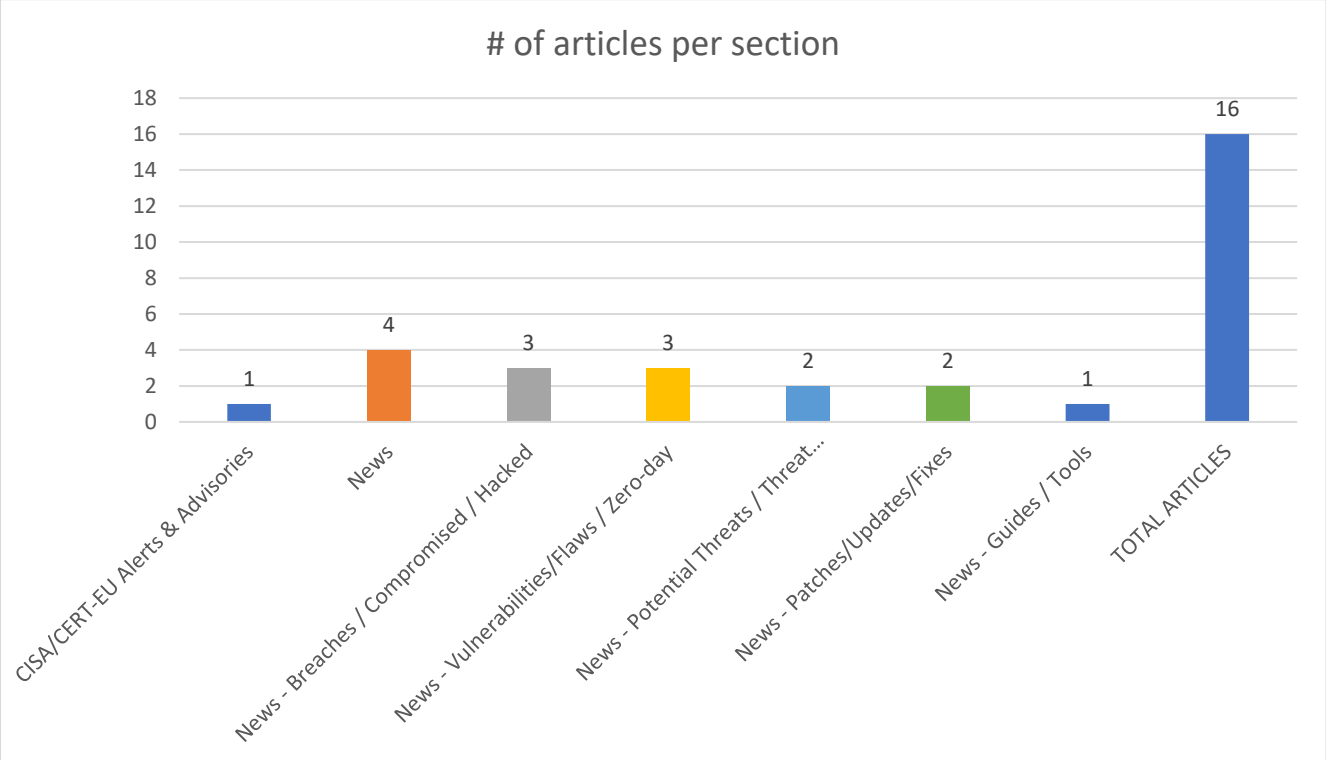
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 07/06/2025 - 10/06/2025





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-2025-5855	9,8	Tenda	Stack-based Buffer Overflow	Tenda AC6 15.03.05.16	https://lavender-bicycle-a5a.notion.site/Tenda-AC6-formsetreboottimer-20a53a41781f80c5b6cac51008556c7e?source=copy_link Exploit Third Party Advisory https://vuldb.com/?ctiid.311601 Permissions Required https://vuldb.com/?id.311601 Third Party Advisory VDB Entry https://vuldb.com/?submit.591422 Third Party Advisory VDB Entry https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-5860	9,8	PHPGurukul Maid Hiring Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/kakalalaww/CVE/issues/2 Exploit Issue Tracking Third Party Advisory https://github.com/kakalalaww/CVE/issues/2 Exploit Issue Tracking Third Party Advisory https://phpgurukul.com/ Product https://vuldb.com/?ctiid.311619 Permissions Required https://vuldb.com/?id.311619 Third Party Advisory VDB Entry https://vuldb.com/?submit.591910
https://nvd.nist.gov/vuln/detail/CVE-2025-5893	9,8	Smart Parking Management System from Honding Technology	Exposure of Sensitive System Information to an Unauthorized Control Sphere		https://www.twcert.org.tw/en/cp-139-10169-651d6-2.html https://www.twcert.org.tw/tw/cp-132-10167-39c6d-1.html

https://nvd.nist.gov/vuln/detail/CVE-2025-5859	8,8	PHPGurukul Nipah Virus Testing Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/f1rstb100d/myCVE/issues/65 Exploit Issue Tracking Third Party Advisory https://github.com/f1rstb100d/myCVE/issues/65 Exploit Issue Tracking Third Party Advisory https://phpgurukul.com/ Product https://vuldb.com/?ctiid.311605 Permissions Required https://vuldb.com/?id.311605 Third Party Advisory VDB Entry https://vuldb.com/?submit.591443
https://nvd.nist.gov/vuln/detail/CVE-2025-5901	8,8	TOTOLINK	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	T10 4.1.8cu.5207	https://candle-throne-f75.notion.site/TOTOLINK-T10-UploadCustomModule-20bdf0aa118580d59961cd545582c118 https://vuldb.com/?ctiid.311674 https://vuldb.com/?id.311674 https://vuldb.com/?submit.592243 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-5934	8,8	Netgear EX3700	Stack-based Buffer Overflow	up to 1.0.0.88	https://github.com/xiaobor123/vul-finds/tree/main/vul-find-ex3700-netgear https://github.com/xiaobor123/vul-finds/tree/main/vul-find-ex3700-netgear#poc https://vuldb.com/?ctiid.311712 https://vuldb.com/?id.311712 https://vuldb.com/?submit.588258 https://www.netgear.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-5912	8,8	D-Link DIR-632 FW103B08	Stack-based Buffer Overflow	D-Link DIR-632 FW103B08	https://github.com/xiaobor123/vul-finds/tree/main/vul-find-dir632-dlink https://github.com/xiaobor123/vul-finds/tree/main/vul-find-dir632-dlink#poc https://vuldb.com/?ctiid.311686 https://vuldb.com/?id.311686 https://vuldb.com/?submit.592307 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-4601	8,8	The "RH - Real Estate WordPress Theme" theme for WordPress	Improper Privilege Management	in all versions up to, and including, 4.4.0.	https://themeforest.net/item/real-homes-wordpress-real-estate-theme/5373914 https://www.wordfence.com/threat-intel/vulnerabilities/id/a816e5a8-2494-4bcf-869d-5214b21f7791?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-4387	8,8	The Abandoned Cart Pro for WooCommerce plugin	Unrestricted Upload of File with Dangerous Type	in all versions up to, and including, 9.16.0.	https://www.tychesoftwares.com/docs/docs/abandoned-cart-pro-for-woocommerce-new/changelog-abandoned-cart-pro/#changelog-abandon-cart-pro-for-woocommerce-9-17-0-release-date-m https://www.tychesoftwares.com/products/woocommerce-abandoned-cart-pro-plugin/ https://www.wordfence.com/threat-intel/vulnerabilities/id/5d2f07bb-89b3-41d4-b606-9722deecf816?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-5837	8,8	PHPGurukul Employee Record Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.3	https://github.com/f1rstb100d/myCVE/issues/61
https://nvd.nist.gov/vuln/detail/CVE-2025-23192	8,2	SAP BusinessObjects Business Intelligence (BI Workspace)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		https://me.sap.com/notes/3560693 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2025-5866	8,0	RT-Thread	Improper Validation of Array Index	5.1.0	https://github.com/RT-Thread/rt-thread/issues/10300 https://vuldb.com/?ctiid.311625 https://vuldb.com/?id.311625 https://vuldb.com/?submit.584127
https://nvd.nist.gov/vuln/detail/CVE-2025-42977	7,6	SAP NetWeaver Visual Composer	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://me.sap.com/notes/3610591 https://url.sap/sapsecuritypatchday

https://nvd.nist.gov/vuln/detail/CVE-2025-42994	7,5	SAP MDM Server ReadString	Free of Memory not on the Heap		https://me.sap.com/notes/3610006 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2025-5870	7,3	TRENDnet	Improper Authentication	TV-IP121W 1.1.1 Build 36	https://github.com/zeke2997/CVE_request_TRENDnet https://vuldb.com/?ctiid.311629 https://vuldb.com/?id.311629 https://vuldb.com/?submit.585435
https://nvd.nist.gov/vuln/detail/CVE-2025-5952	7,3	Zend	Improper Neutralization of Special Elements used in a Command ('Command Injection')	To up to 6.10-6 Beta	https://matheuscezar.github.io/2025/05/24/0-day-in-zend-to.html https://vuldb.com/?ctiid.311789 https://vuldb.com/?id.311789 https://vuldb.com/?submit.589178
https://nvd.nist.gov/vuln/detail/CVE-2025-5906	7,3	Laundry System	Improper Authentication	1.0	https://code-projects.org/ https://github.com/tuooo/CVE/issues/11 https://vuldb.com/?ctiid.311679 https://vuldb.com/?id.311679 https://vuldb.com/?submit.592266
https://nvd.nist.gov/vuln/detail/CVE-2025-5840	7,3	Source-Codester Client Database Management System	Improper Access Control	1.0	https://github.com/592833263/cve/issues/1 https://vuldb.com/?ctiid.311583 https://vuldb.com/?id.311583 https://vuldb.com/?submit.591425 https://www.sourcecodester.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-5303	7,2	The LTL Freight Quotes – Freightview Edition, LTL Freight Quotes – Daylight Edition and LTL Freight Quotes – Day & Ross Edition plugins for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	in all versions up to, and including, 1.0.11, 2.2.6 and 2.1.10	https://plugins.trac.wordpress.org/browser/ltl-freight-quotes-day-ross-edition/trunk/en-hit-to-update-plan.php#L29 https://plugins.trac.wordpress.org/browser/ltl-freight-quotes-daylight-edition/tags/2.2.6/en-hit-to-update-plan.php#L29 https://plugins.trac.wordpress.org/browser/ltl-freight-quotes-freightview-edition/tags/1.0.11/common/en-plans.php#L110 https://plugins.trac.wordpress.org/browser/ltl-freight-quotes-freightview-edition/tags/1.0.11/en-hit-to-update-plan.php#L29 https://www.wordfence.com/threat-intel/vulnerabilities/id/05fc4b17-7922-45a4-aac8-a47b3f50ce69?source=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-32433 Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability ▪ CVE-2024-42009 RoundCube Webmail Cross-Site Scripting Vulnerability	https://www.cisa.gov/news-events/alerts/2025/06/09/cisa-adds-two-known-exploited-vulnerabilities-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
China-linked threat actor targeted +70 orgs worldwide, SentinelOne warns	https://securityaffairs.com/178819/apt/china-linked-threat-actor-targeted-70-orgs-worldwide-sentinelone-warns.html
Linux Foundation unveils decentralized WordPress plugin manager	https://www.bleepingcomputer.com/news/technology/linux-foundation-unveils-decentralized-wordpress-plugin-manager/
Trump Administration Revises Cybersecurity Rules, Replaces Biden and Obama Orders	https://www.infosecurity-magazine.com/news/trump-new-cyber-executive-order/
OpenAI Bans ChatGPT Accounts Used by Russian, Iranian, and Chinese Hacker Groups	https://thehackernews.com/2025/06/openai-bans-chatgpt-accounts-used-by.html

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Malicious Browser Extensions Infect Over 700 Users Across Latin America Since Early 2025	https://thehackernews.com/2025/06/malicious-browser-extensions-infect-722.html
Experts found 4 billion user records online, the largest known leak of Chinese personal data from a single source	https://securityaffairs.com/178744/data-breach/experts-found-4-billion-user-records-online-the-largest-known-leak-of-chinese-personal-data-from-a-single-source.html
Tax resolution firm Optima Tax Relief hit by ransomware, data leaked	https://www.bleepingcomputer.com/news/security/tax-resolution-firm-optima-tax-relief-hit-by-ransomware-data-leaked/?&web_view=true

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Over 84,000 Roundcube instances vulnerable to actively exploited flaw	**https://www.bleepingcomputer.com/news/security/over-84-000-roundcube-instances-vulnerable-to-actively-exploited-flaw/**
PayU Plugin Flaw Allows Account Takeover on 5000 WordPress Sites	https://www.infosecurity-magazine.com/news/payu-plugin-flaw-wordpress-account/
New Mirai botnet infect TBK DVR devices via command injection flaw	https://www.bleepingcomputer.com/news/security/new-mirai-botnet-infect-tbk-dvr-devices-via-command-injection-flaw/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Google patched bug leaking phone numbers tied to accounts	**https://www.bleepingcomputer.com/news/security/google-patched-bug-leaking-phone-numbers-tied-to-accounts/**
Week in review: Google fixes exploited Chrome zero-day, Patch Tuesday forecast	https://www.helpnetsecurity.com/2025/06/08/week-in-review-google-fixes-exploited-chrome-zero-day-patch-tuesday-forecast/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
FBI Warns Smart Home Users of Badbox 2.0 Botnet Threat	**https://www.infosecurity-magazine.com/news/fbi-smart-home-users-badbox-20/**
New Mirai botnet targets TBK DVRs by exploiting CVE-2024-3721	https://securityaffairs.com/178779/malware/new-mirai-botnet-targets-tbk-dvrs-by-exploiting-cve-2024-3721.html

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/