NATIONAL CYBERSECURITY AUTHORITY GR

CVEs Alerts

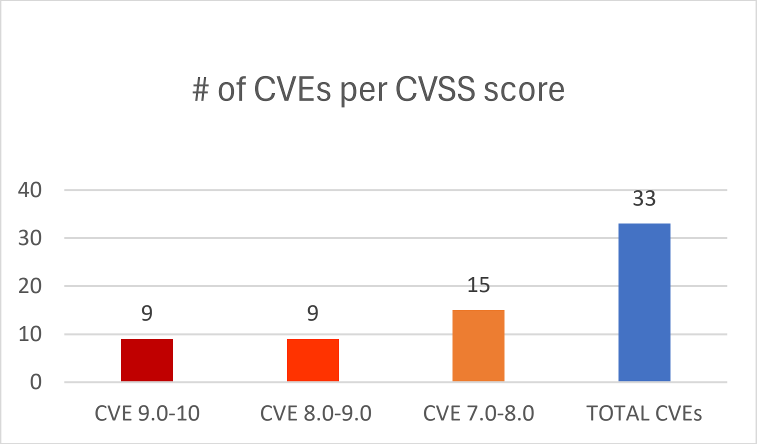
CVEs, CISA/CERT-EU
Alerts
Advisories
& News

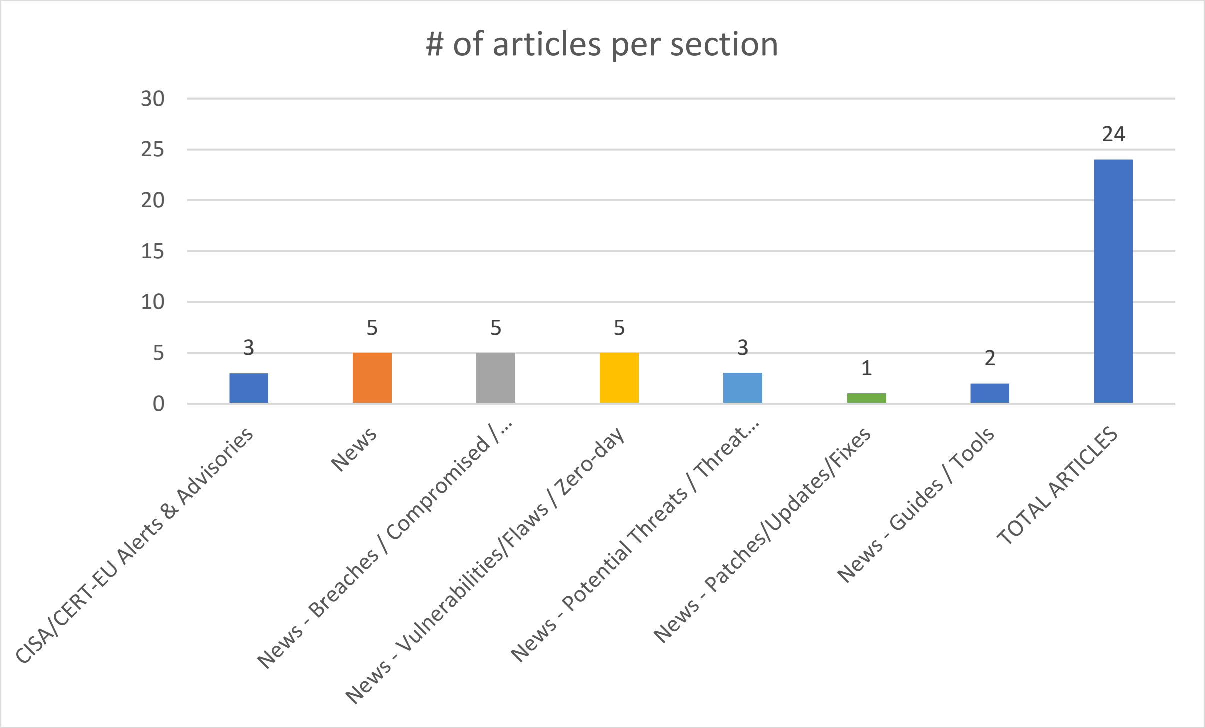
Newsletter on system vulnerabilities and cybersecurity news

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 21/05/2025 - 23/05/2025





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-2025-48200	**10,0**	The sr_feuser_register extension	Deserialization of Untrusted Data	through 12.4.8 for TYPO3	https://typo3.org/security/advisory/typo3-ext-sa-2025-008
https://nvd.nist.gov/vuln/detail/CVE-2025-36535	**10,0**	The embedded web server	Missing Authentication for Critical Function		https://www.automationdirect.com/adc/shopping/catalog/communications/protocol_gateways/modbus_gateways/eki-1221-ce https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-09
https://nvd.nist.gov/vuln/detail/CVE-2025-44880	**9,8**	Wavlink WL-WN579A3	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	v1.0	https://lafdrew.github.io/2025/03/27/Remote-Command-Execution-in-adm-cgi-of-wavlink-WL-WN579A3-Device/
https://nvd.nist.gov/vuln/detail/CVE-2025-44883	**9,8**	FW-WGS-804HPT	Stack-based Buffer Overflow	v1.305b241111	https://lafdrew.github.io/2025/04/20/web-tacplus-serverEdit-post-taclp/
https://nvd.nist.gov/vuln/detail/CVE-2025-4094	**9,8**	The DIGITS: WordPress Mobile Number Signup and Login WordPress plugin		before 8.4.6.1	https://wpscan.com/vulnerability/b5f0a263-644b-4954-a1f0-d08e2149edbb/
https://nvd.nist.gov/vuln/detail/CVE-2025-4524	**9,8**	The Madara – Responsive and modern WordPress theme for manga sites	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 2.2.2	https://mangabooth.com/product/wp-manga-theme-madara/ https://www.wordfence.com/threat-intel/vulnerabilities/id/a3ee01da-218a-421d-8f9c-1dc6c056ef74?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-41426	**9,8**	Vertiv products	Stack-based Buffer Overflow		https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-10 https://www.vertiv.com/en-us/support/security-support-center/
https://nvd.nist.gov/vuln/detail/CVE-2025-3483	**9,8**	MedDream PACS Server DICOM File	Stack-based Buffer Overflow		https://www.zerodayinitiative.com/advisories/ZDI-25-243/
https://nvd.nist.gov/vuln/detail/CVE-2025-41232	**9,1**	Spring Security Aspects	Protection Mechanism Failure		http://spring.io/security/cve-2025-41232
https://nvd.nist.gov/vuln/detail/CVE-2025-3882	**8,8**	eCharge Hardy Barth cPH2 nwcheckexec.php	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://www.zerodayinitiative.com/advisories/ZDI-25-248/
https://nvd.nist.gov/vuln/detail/CVE-2025-3887	**8,8**	GStreamer	Stack-based Buffer Overflow	GStreamer H265	https://www.zerodayinitiative.com/advisories/ZDI-25-267/
https://nvd.nist.gov/vuln/detail/CVE-2024-25010	**8,8**	Ericsson	Improper Input Validation	Ericsson RAN Compute and Site Controller 6610	https://www.ericsson.com/en/about-us/security/psirt/CVE-2024-25010
https://nvd.nist.gov/vuln/detail/CVE-2025-48201	**8,6**	The ns_backup extension	Direct Request ('Forced Browsing')	through 13.0.0 for TYPO3	https://typo3.org/security/advisory/typo3-ext-sa-2025-007
https://nvd.nist.gov/vuln/detail/CVE-2025-48207	**8,6**	The reint_downloadmanager extension	Direct Request ('Forced Browsing')	through 5.0.0 for TYPO3	https://typo3.org/security/advisory/typo3-ext-sa-2025-004
https://nvd.nist.gov/vuln/detail/CVE-2025-20152	**8,6**	RADIUS message processing feature of Cisco Identity Services Engine (ISE)	Out-of-bounds Read		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-restart-ss-uf986G2Q

https://nvd.nist.gov/vuln/detail/CVE-2025-27997	**8,4**	Blizzard Battle.net	Uncontrolled Search Path Element	v2.40.0.15267	https://gist.github.com/sornram9254/4593dd5eb2bcca50d68dc6ac70e40b24
https://nvd.nist.gov/vuln/detail/CVE-2025-27998	**8,4**	Valvesoftware Steam Client	Improper Control of Generation of Code ('Code Injection')	Steam Client 1738026274	https://gist.github.com/sornram9254/e8d10efcf246cc50ff3d4f837b261616
https://nvd.nist.gov/vuln/detail/CVE-2025-3836	**8,3**	Zohocorp ManageEngine ADAudit Plus	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	versions 8510 and prior	https://www.manageengine.com/products/active-directory-audit/cve-2025-3836.html
https://nvd.nist.gov/vuln/detail/CVE-2025-48413	**7,7**	\`/etc/passwd\` and \`/etc/shadow\` files	Use of Hard-coded Credentials		https://r.sec-consult.com/echarge
https://nvd.nist.gov/vuln/detail/CVE-2024-56429	**7,7**	itech iLabClient	Use of Hard-coded Cryptographic Key	itech iLabClient 3.7.1	https://github.com/lisa-2905/CVE-2024-56429 https://itech-gmbh.de/produkte/
https://nvd.nist.gov/vuln/detail/CVE-2025-3486	**7,7**	Allegra isZipEntryValide	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://alltena.com/en/resources/release-notes/release-notes-for-release-8-1-2 https://www.zerodayinitiative.com/advisories/ZDI-25-255/
https://nvd.nist.gov/vuln/detail/CVE-2025-4123	**7,6**	Grafana	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		https://grafana.com/security/security-advisories/cve-2025-4123/
https://nvd.nist.gov/vuln/detail/CVE-2025-40775	**7,5**	BIND	Improper Handling of Undefined Values	BIND 9 versions 9.20.0 through 9.20.8 and 9.21.0 through 9.21.7	http://www.openwall.com/lists/oss-security/2025/05/21/1 https://kb.isc.org/docs/cve-2025-40775
https://nvd.nist.gov/vuln/detail/CVE-2025-4416	**7,5**	Events Log Track	Allocation of Resources Without Limits or Throttling	from 0.0.0 before 3.1.11, from 4.0.0 before 4.0.2	https://www.drupal.org/sa-contrib-2025-059

https://nvd.nist.gov/vuln/detail/CVE-2025-47947	**7,5**	ModSecurity	Excessive Platform Resource Consumption within a Loop	Versions up to and including 2.9.8	https://github.com/owasp-modsecurity/ModSecurity/pull/3389 https://github.com/owasp-modsecurity/ModSecurity/security/advisories/GHSA-859r-vvv8-rm8r https://github.com/owasp-modsecurity/ModSecurity/security/advisories/GHSA-859r-vvv8-rm8r
https://nvd.nist.gov/vuln/detail/CVE-2025-3884	**7,5**	Cloudera Hue Ace Editor Directory	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://www.zerodayinitiative.com/advisories/ZDI-25-250/
https://nvd.nist.gov/vuln/detail/CVE-2025-5002	**7,3**	SourceCodester Client Database Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/laifeng-boy/cve/issues/5 https://github.com/laifeng-boy/cve/issues/5 https://vuldb.com/?ctiid.309657 https://vuldb.com/?id.309657 https://vuldb.com/?submit.580192 https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-5003	**7,3**	Online Time Table Generator	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/huangyi234/CVE/issues/4 https://github.com/huangyi234/CVE/issues/4 https://vuldb.com/?ctiid.309658 https://vuldb.com/?id.309658 https://vuldb.com/?submit.580195
https://nvd.nist.gov/vuln/detail/CVE-2025-5006	**7,3**	Campcodes Online Shopping Portal	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/Zhaozhizhi/CVE/issues/3 https://github.com/Zhaozhizhi/CVE/issues/3 https://vuldb.com/?ctiid.309660 https://vuldb.com/?id.309660 https://vuldb.com/?submit.580248 https://www.campcodes.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-5049	**7,3**	FreeFloat FTP Server	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1.0	https://fitoxs.com/exploit/e837c056f1ced605a9574541c7bf9861982bbf52ac5da3a5c5b637dbbadb49b7-exploit.txt https://vuldb.com/?ctiid.309868 https://vuldb.com/?id.309868 https://vuldb.com/?submit.581278
https://nvd.nist.gov/vuln/detail/CVE-2025-4803	**7,2**	The Glossary by WPPedia – Best Glossary plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 1.3.0	https://github.com/bfiessinger/wppedia/blob/1d0b8568349c9c9479372f845a812eb2aa4b3d09/core/classes/traits/trait-sanitizes-data.php#L64 https://plugins.trac.wordpress.org/browser/wppedia/tags/1.3.0/core/classes/class-options.php#L396 https://plugins.trac.wordpress.org/browser/wppedia/tags/1.3.0/core/classes/traits/trait-sanitizes-data.php#L64 https://www.wordfence.com/threat-intel/vulnerabilities/id/53fb54bc-6eaa-4e99-a41c-e59a9bae81e5?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-20113	**7,1**	Cisco Unified Intelligence Center	Client-Side Enforcement of Server-Side Security		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuis-priv-esc-3Pk96SU4
https://nvd.nist.gov/vuln/detail/CVE-2025-2759	**7,0**	GStreamer	Incorrect Permission Assignment for Critical Resource		https://www.zerodayinitiative.com/advisories/ZDI-25-268/

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Advisory Update on Cyber Threat Activity Targeting Commvault's SaaS Cloud Application (Metallic)		https://www.cisa.gov/news-events/alerts/2025/05/22/advisory-update-cyber-threat-activity-targeting-commvaults-saas-cloud-application-metallic
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-4632 Samsung MagicINFO 9 Server Path Traversal Vulnerability	https://www.cisa.gov/news-events/alerts/2025/05/22/cisa-adds-one-known-exploited-vulnerability-catalog
New Best Practices Guide for Securing AI Data Released		https://www.cisa.gov/news-events/alerts/2025/05/22/new-best-practices-guide-securing-ai-data-released

News

Σύντομη περιγραφή / Τίτλος	URL
Police takes down 300 servers in ransomware supply-chain crackdown	https://www.bleepingcomputer.com/news/security/police-takes-down-300-servers-in-ransomware-supply-chain-crackdown/
#Infosec2025: NCC Group Expert Warns UK Firms to Prepare for Cyber Security and Resilience Bill	https://www.infosecurity-magazine.com/news/infosec2025-ncc-uk-cybersecurity/
CISA Warns of Suspected Broader SaaS Attacks Exploiting App Secrets and Cloud Misconfigs	https://thehackernews.com/2025/05/cisa-warns-of-suspected-broader-saas.html
Coca-Cola, Bottling Partner Named in Separate Ransomware and Data Breach Claims	https://hackread.com/coca-cola-bottling-partner-ransomware-data-breach/
Microsoft dials up Uncle Sam to take down LummaC2 malware backbone	https://scmagazine.com/news/microsoft-dials-up-uncle-sam-to-take-down-lummac2-malware-backbone

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Chinese threat actors exploited Trimble Cityworks flaw to breach U.S. local government networks	https://securityaffairs.com/178203/hacking/chinese-threat-actors-exploited-trimble-cityworks-flaw-to-breach-u-s-local-government-networks.html
Over 100 Malicious Chrome Extensions Found Stealing User Data Through Spoofed VPN and Productivity Tools	https://dailysecurityreview.com/security-spotlight/over-100-malicious-chrome-extensions-found-stealing-user-data-through-spoofed-vpn-and-productivity-tools/
Sensitive Personal Data Stolen in West Lothian Ransomware Attack	https://www.infosecurity-magazine.com/news/personal-data-stolen-west-lothian/
Database Leak Reveals 184 Million Infostealer-Harvested Emails and Passwords	https://hackread.com/database-leak-184-million-infostealer-emails-passwords/
Coinbase Breach Affected Almost 70,000 Customers	https://www.infosecurity-magazine.com/news/coinbase-breach-affected-almost/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Unpatched Windows Server vulnerability allows full domain compromise	**https://www.helpnetsecurity.com/2025/05/22/unpatched-windows-server-vulnerability-allows-active-directory-users-full-domain-compromise/**
Ivanti EPMM flaw exploited by Chinese hackers to breach govt agencies	https://www.bleepingcomputer.com/news/security/ivanti-epmm-flaw-exploited-by-chinese-hackers-to-breach-govt-agencies/
Flaw in Google Cloud Functions Sparks Broader Security Concerns	https://www.infosecurity-magazine.com/news/flaw-google-cloud-security-concerns/
Critical Windows Server 2025 dMSA Vulnerability Enables Active Directory Compromise	https://thehackernews.com/2025/05/critical-windows-server-2025-dmsa.html
Critical Versa Concerto Flaws Let Attackers Escape Docker and Compromise Hosts	https://thehackernews.com/2025/05/unpatched-versa-concerto-flaws-let.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
ThreatLocker Patch Management: A Security-First Approach to Closing Vulnerability Windows	**https://www.bleepingcomputer.com/news/security/threatlocker-patch-management-a-security-first-approach-to-closing-vulnerability-windows/**

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
DragonForce Engages in "Turf War" for Ransomware Dominance	https://www.infosecurity-magazine.com/news/dragonforce-turf-war-ransomware/
Cybercriminals Mimic Kling AI to Distribute Infostealer Malware	https://www.infosecurity-magazine.com/news/cyber-criminals-mimic-kling-ai/
GitLab's AI Assistant Opened Devs to Code Theft	https://www.darkreading.com/application-security/gitlab-ai-assistant-opened-devs-to-code-theft

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/