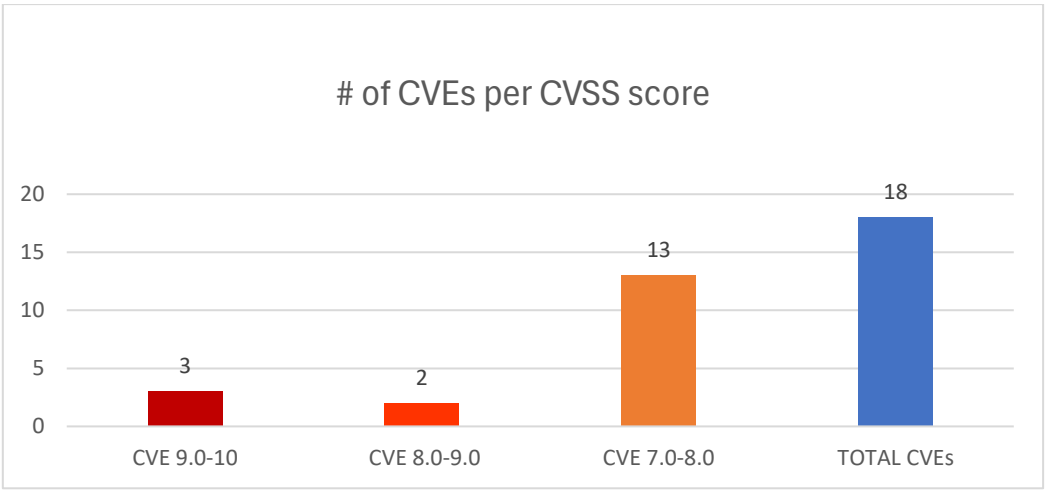
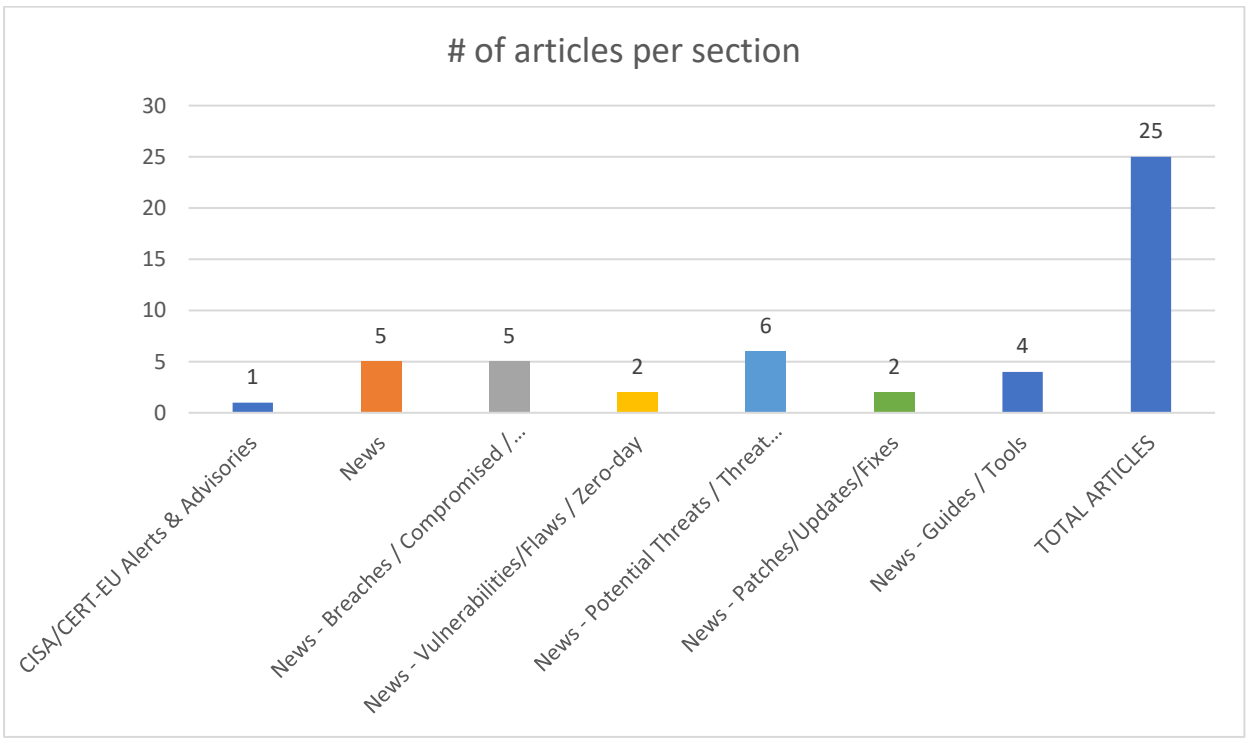
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 03/05/2025 - 06/05/2025





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-2025-0782	**10**	S3 bucket configuration for h2oai/h2o-3	Missing Authorization	all versions	https://github.com/h2oai/h2o-3/commit/6740655b70cef40ec67d952bee2d23f7d33c7419 https://huntr.com/bounties/4587cec7-8bc5-48ab-8614-105d41c99151
https://nvd.nist.gov/vuln/detail/CVE-2025-3918	**9,8**	The Job Listings plugin for WordPress	Improper Authorization	in versions 0.1 to 0.1.1	https://plugins.trac.wordpress.org/browser/job-listings/trunk/includes/forms/class-jlt-form-member.php#L68 https://wordpress.org/plugins/job-listings/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/c9cd43f5-c3d0-4eb2-9c18-1af2edca37ff?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-2905	**9,1**	WSO2 API Manager	Improper Restriction of XML External Entity Reference	On systems running JDK 7 or early JDK 8	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2025/WSO2-2025-3993/
https://nvd.nist.gov/vuln/detail/CVE-2025-3610	**8,8**	The Reales WP STPT plugin for WordPress	Authorization Bypass Through User-Controlled Key	all versions up to, and including, 2.1.2	https://themeforest.net/item/reales-wp-real-estate-wordpress-theme/10330568 https://www.wordfence.com/threat-intel/vulnerabilities/id/38c6b149-39d7-491a-9f3a-261087a52a03?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-47245	**8,1**	BlueWave Checkmate	External Control of Assumed-Immutable Web Parameter	version 2.0.2	https://github.com/bluewave-labs/Checkmate/commit/d4a60723f490502b3fe6f7f780a85d29bf5d1385 https://github.com/bluewave-labs/Checkmate/pull/2160 https://github.com/bluewave-labs/Checkmate/security/advisories/GHSA-7x3q-g6gq-f4mm
https://nvd.nist.gov/vuln/detail/CVE-2025-4226	**7,3**	PHPGurukul Cyber Cafe Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/diyuzhishen/mycve/issues/2 https://phpgurukul.com/ https://vuldb.com/?ctiid.307323 https://vuldb.com/?id.307323 https://vuldb.com/?submit.562409
https://nvd.nist.gov/vuln/detail/CVE-2025-4236	**7,3**	PCMan FTP Server	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	version 2.0.7	https://fitoxs.com/exploit/exploit-900150983cd24fb0d6963f7d28e17f72.txt https://vuldb.com/?ctiid.307327 https://vuldb.com/?id.307327 https://vuldb.com/?submit.561510
https://nvd.nist.gov/vuln/detail/CVE-2025-4242	**7,3**	PHPGurukul Online Birth Certificate System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 2.0	https://github.com/bluechips-zhao/myCVE/issues/8 https://phpgurukul.com/ https://vuldb.com/?ctiid.307333 https://vuldb.com/?id.307333 https://vuldb.com/?submit.562624
https://nvd.nist.gov/vuln/detail/CVE-2025-4265	**7,3**	PHPGurukul Emergency Ambulance Hiring Portal	Improper Neutralization of Special Elements used in an SQL	version 1.0	https://github.com/xiguala123/myCVE/issues/2 https://phpgurukul.com/ https://vuldb.com/?ctiid.307369

			Command ('SQL Injection')		https://vuldb.com/?id.307369 https://vuldb.com/?submit.562993
https://nvd.nist.gov/vuln/detail/CVE-2025-4263	**7,3**	PHPGurukul Online DJ Booking Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/MoshangChunfeng/CVE/issues/2 https://phpgurukul.com/ https://vuldb.com/?ctiid.307367 https://vuldb.com/?id.307367 https://vuldb.com/?submit.562991
https://nvd.nist.gov/vuln/detail/CVE-2025-4312	**7,3**	SourceCodester Advanced Web Store	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/Samsamue1/CVE/issues/1 https://vuldb.com/?ctiid.307415 https://vuldb.com/?id.307415 https://vuldb.com/?submit.564301 https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-4311	**7,3**	Content Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/ZhaoxuepengS/CVE-vul/issues/2 https://itsourcecode.com/ https://vuldb.com/?ctiid.307414 https://vuldb.com/?id.307414 https://vuldb.com/?submit.564230
https://nvd.nist.gov/vuln/detail/CVE-2025-4314	**7,3**	SourceCodester Advanced Web Store	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/Samsamue1/CVE/issues/3 https://vuldb.com/?ctiid.307417 https://vuldb.com/?id.307417 https://vuldb.com/?submit.564314 https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-2802	**7,3**	The LayoutBoxx plugin for WordPress	Improper Control of Generation of	all versions up to, and including, 0.3.1	https://plugins.svn.wordpress.org/layoutboxx/trunk/layoutboxx.php

			Code ('Code Injection')		https://wordpress.org/plugins/layoutboxx/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/fc3fcb8f-f130-4008-8f11-d98efa30f1a8?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-4309	**7,3**	PHPGurukul Art Gallery Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.1	https://github.com/lierran1/CVE/issues/3 https://phpgurukul.com/ https://vuldb.com/?ctiid.307412 https://vuldb.com/?id.307412 https://vuldb.com/?submit.564207
https://nvd.nist.gov/vuln/detail/CVE-2025-4306	**7,3**	PHPGurukul Nipah Virus Testing Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/xiguala123/myCVE/issues/3 https://phpgurukul.com/ https://vuldb.com/?ctiid.307409 https://vuldb.com/?id.307409 https://vuldb.com/?submit.564120
https://nvd.nist.gov/vuln/detail/CVE-2025-4304	**7,3**	PHPGurukul Cyber Cafe Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/3507998897/myCVE/issues/3 https://phpgurukul.com/ https://vuldb.com/?ctiid.307407 https://vuldb.com/?id.307407 https://vuldb.com/?submit.563723
https://nvd.nist.gov/vuln/detail/CVE-2025-4303	**7,3**	PHPGurukul Human Metapneumovirus Testing Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/eneover/myCVE/issues/1 https://phpgurukul.com/ https://vuldb.com/?ctiid.307406 https://vuldb.com/?id.307406 https://vuldb.com/?submit.563706

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-3248 Langflow Missing Authentication Vulnerability	https://www.cisa.gov/news-events/alerts/2025/05/05/cisa-adds-one-known-exploited-vulnerability-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
How cybercriminals exploit psychological triggers in social engineering attacks	https://www.helpnetsecurity.com/2025/05/06/social-engineering-human-behavior/
Commvault CVE-2025-34028 Added to CISA KEV After Active Exploitation Confirmed	https://thehackernews.com/2025/05/commvault-cve-2025-34028-added-to-cisa.html
Dissecting the 2025 Microsoft Vulnerabilities Report: Key Trends and Insights	https://thehackernews.com/expert-insights/2025/05/dissecting-2025-microsoft.html
How OSINT supports financial crime investigations	https://www.helpnetsecurity.com/2025/05/05/stuart-clarke-blackdot-solutions-financial-crime-osint/
U.S. CISA adds Yii Framework and Commvault Command Center flaws to its Known Exploited Vulnerabilities catalog	https://securityaffairs.com/177367/hacking/u-s-cisa-adds-yii-framework-and-commvault-command-center-flaws-to-its-known-exploited-vulnerabilities-catalog.html

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Darcula PhaaS steals 884,000 credit cards via phishing texts	https://www.bleepingcomputer.com/news/security/darcula-phaas-steals-884-000-credit-cards-via-phishing-texts/
Kelly Benefits December data breach impacted over 400,000 individuals	https://securityaffairs.com/177476/data-breach/kelly-benefits-december-data-breach-impacted-over-400000-individuals.html
UK retailers under cyber attack: Co-op member data compromised	https://www.helpnetsecurity.com/2025/05/05/uk-retailers-under-cyber-attack-co-op-member-data-compromised/
A hacker stole data from TeleMessage, the firm that sells modified versions of Signal to the U.S. gov	https://securityaffairs.com/177458/hacking/a-hacker-stole-data-from-telemessage-the-firm-that-sells-modified-versions-of-signal-to-the-u-s-gov.html
beWanted Exposes Personal Data of 1.1 Million Job Seekers Across Europe and Latin America	https://dailysecurityreview.com/security-spotlight/bewanted-exposes-personal-data-of-1-1-million-job-seekers-across-europe-and-latin-america/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Week in review: Critical SAP NetWeaver flaw exploited, RSAC 2025 Conference	https://www.helpnetsecurity.com/2025/05/04/week-in-review-critical-sap-netweaver-flaw-exploited-rsac-2025-conference/
Billions of Apple Devices at Risk from “AirBorne” AirPlay Vulnerabilities	https://hackread.com/apple-devices-risk-airborne-airplay-vulnerabilities/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Update ASAP: Google Fixes Android Flaw (CVE-2025-27363) Exploited by Attackers	https://thehackernews.com/2025/05/google-fixes-actively-exploited-android.html
Microsoft silently fixes Start menu bug affecting Windows 10 PCs	https://www.bleepingcomputer.com/news/microsoft/microsoft-silently-fixes-start-menu-bug-affecting-windows-10-pcs/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Microsoft finds default Kubernetes Helm charts can expose data	https://www.bleepingcomputer.com/news/security/microsoft-finds-default-kubernetes-helm-charts-can-expose-data/
StealC Malware Upgraded With Advanced Data Theft and Stealth Capabilities	https://dailysecurityreview.com/security-spotlight/stealc-malware-upgraded-with-advanced-data-theft-and-stealth-capabilities/
Chinese Group TheWizards Exploits IPv6 to Drop WizardNet Backdoor	https://hackread.com/chinese-thewizards-exploits-ipv6-wizardnet-backdoor/
Golden Chickens Deploy TerraStealerV2 to Steal Browser Credentials and Crypto Wallet Data	https://thehackernews.com/2025/05/golden-chickens-deploy-terrastealerv2.html
Malicious Go Modules designed to wipe Linux systems	https://securityaffairs.com/177411/malware/malicious-go-modules-designed-to-wipe-linux-systems.html
Phishing Emails Impersonating Qantas Target Credit Card Info	https://hackread.com/phishing-emails-impersonate-qantas-credit-card-info/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best Cyber Attack Simulation Tools – 2025	https://cybersecuritynews.com/cyber-attack-simulation-tools/
The ultimate guide to SaaS identity security in 2025	https://thehackernews.uk/saas-identity-guide-25
10 Steps to Microsoft 365 Cyber Resilience	https://thehackernews.uk/m365-cyber-resilience-10
Top Cybersecurity Tools of 2025 To Managing Remote Device Threats	https://cybersecuritynews.com/top-cybersecurity-tools-managing-remote-device-threats/

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/