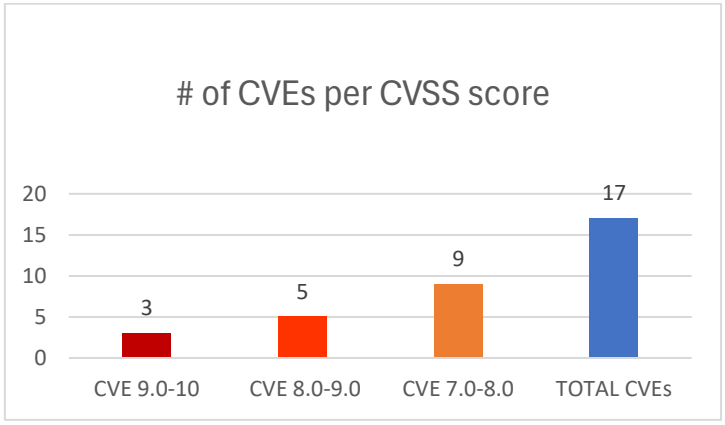
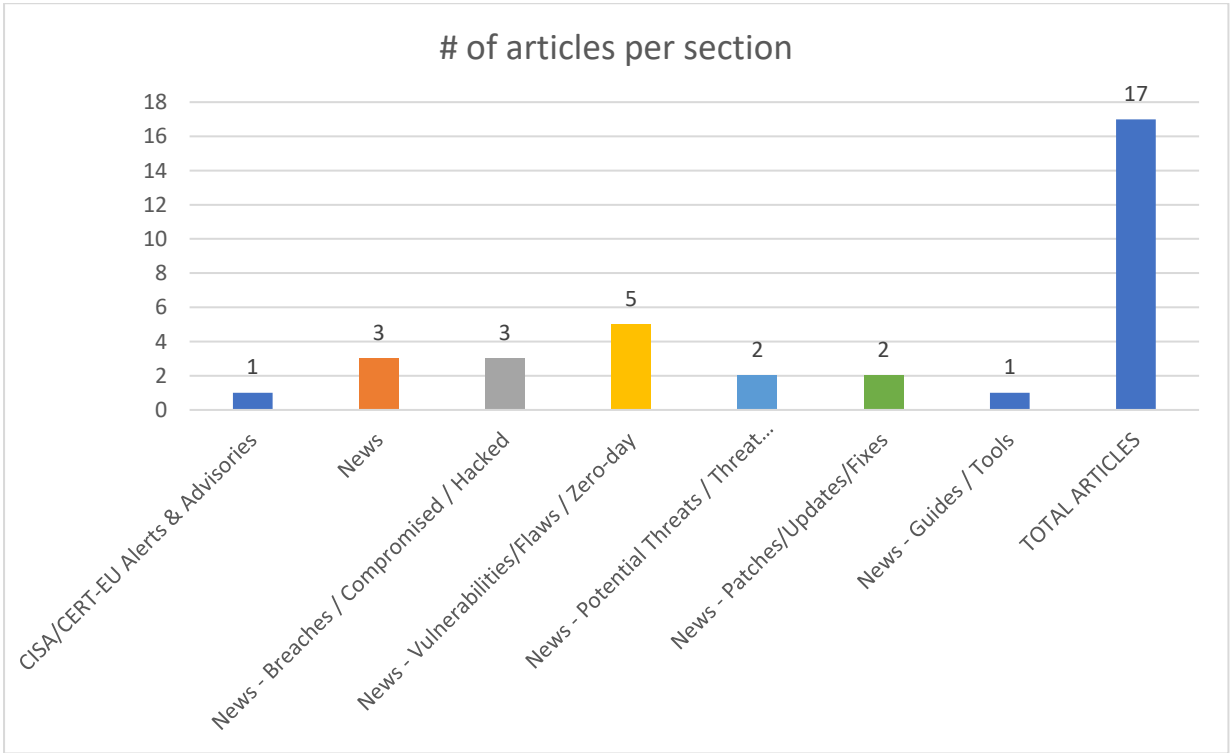
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 31/05/2025 - 03/06/2025





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 7
News 7
Breaches / Compromised / Hacked 7
Vulnerabilities / Flaws / Zero-day 8
Patches / Updates / Fixes 8
Potential threats / Threat intelligence 8
Guides / Tools 8
References 9
Annex – Websites with vendor specific vulnerabilities 10

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-2025-5086	10,0	DELMIA Apriso	Deserialization of Untrusted Data	from Release 2020 through Release 2025Â	https://www.3ds.com/vulnerability/advisories
https://nvd.nist.gov/vuln/detail/CVE-2025-4631	9,8	The Profitori plugin for WordPress	Improper Authorization	versions 2.0.6.0 to 2.1.1.3	https://plugins.trac.wordpress.org/browser/profitori/tags/2.1.1.3/profitori.php#L2675 https://plugins.trac.wordpress.org/browser/profitori/tags/2.1.1.3/profitori.php#L2679 https://plugins.trac.wordpress.org/browser/profitori/tags/2.1.1.3/profitori.php#L2698 https://plugins.trac.wordpress.org/browser/profitori/tags/2.1.1.3/profitori.php#L3673 https://wordpress.org/plugins/profitori/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/c764811f-e9dc-4c3d-b696-5792e70ff0b6?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-4607	9,8	The PSW Front-end Login & Registration plugin for WordPress	Use of Insufficiently Random Values	all versions up to, and including, 1.12	https://plugins.trac.wordpress.org/browser/psw-login-and-registration/trunk/public/class-prositegeneralfeatures-public.php#L323 https://plugins.trac.wordpress.org/browser/psw-login-and-registration/trunk/public/class-prositegeneralfeatures-public.php#L493 https://plugins.trac.wordpress.org/browser/psw-login-and-registration/trunk/public/class-prositegeneralfeatures-public.php#L731 https://wordpress.org/plugins/psw-login-and-registration/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/a2d6e595-0682-4a41-a432-afbcb50144e8?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-4672	8,8	The Offsprout Page Builder plugin for WordPress	Improper Authorization	versions 2.2.1 to 2.15.2	https://plugins.trac.wordpress.org/browser/offsprout-page-builder/tags/2.15.2/api/class-offsprout-api-extensions.php#L5 https://plugins.trac.wordpress.org/browser/offsprout-page-builder/tags/2.15.2/api/class-offsprout-api-extensions.php#L514 https://wordpress.org/plugins/offsprout-page-builder/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/9269d18d-8d83-43ff-b777-ba8f58321e9e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-4103	8,8	The WP-GeoMeta plugin for WordPress	Improper Authorization	versions 0.3.4 to 0.3.5	https://plugins.trac.wordpress.org/browser/wp-geometa/tags/0.3.4/lib/wp-geometa-dash.php#L896 https://wordpress.org/plugins/wp-geometa/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/43039f2a-b3f9-4836-8b55-e8a091b1a102?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-1051	8,8	Sonos Era 300	Heap-based Buffer Overflow	Sonos Era 300	https://www.zerodayinitiative.com/advisories/ZDI-25-311/
https://nvd.nist.gov/vuln/detail/CVE-2024-57783	8,1	Dot	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	0.9.3	https://dotapp.uk https://github.com/EDMPL/Vulnerability-Research/tree/main/CVE-2024-57783 https://github.com/alexpinel/Dot/issues/28
https://nvd.nist.gov/vuln/detail/CVE-2025-20298	8,0	Universal Forwarder for Windows	Incorrect Permission Assignment for Critical Resource	versions below 9.4.2, 9.3.4, 9.2.6, and 9.1.9	https://advisory.splunk.com/advisories/SVD-2025-0602
https://nvd.nist.gov/vuln/detail/CVE-2025-26396	7,8	The SolarWinds Dameware Mini Remote Control	Improper Privilege Management		https://documentation.solarwinds.com/en/success_center/dameware/content/release_notes/dameware_12-3-2_release_notes.htm https://www.solarwinds.com/trust-center/security-advisories/CVE-2025-26396
https://nvd.nist.gov/vuln/detail/CVE-2025-5036	7,8	Autodesk Revit	Use After Free		https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0009

https://nvd.nist.gov/vuln/detail/CVE-2025-27956	7,5	WebLaudos	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24.2 (04)	https://github.com/intruderlabs/cvex/blob/main/Pixeon/WebLaudos/Directory-Traversal/README.md
https://nvd.nist.gov/vuln/detail/CVE-2025-5371	7,3	Source-Codester Health Center Patient Record Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/shanranne/myCVE/issues/4 https://vuldb.com/?ctiid.310664 https://vuldb.com/?id.310664 https://vuldb.com/?submit.587382 https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-5370	7,3	PHPGurukul News Portal	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	4.1	https://github.com/GarminYoung/myCVE/issues/5 https://phpgurukul.com/ https://vuldb.com/?ctiid.310663 https://vuldb.com/?id.310663 https://vuldb.com/?submit.587365
https://nvd.nist.gov/vuln/detail/CVE-2025-5369	7,3	SourceCodester PHP Display Username After Login	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/shanranne/myCVE/issues/2 https://vuldb.com/?ctiid.310662 https://vuldb.com/?id.310662 https://vuldb.com/?submit.587234 https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-5367	7,3	PHPGurukul Online Shopping Portal Project	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/shanranne/myCVE/issues/1 https://phpgurukul.com/ https://vuldb.com/?ctiid.310660 https://vuldb.com/?id.310660 https://vuldb.com/?submit.586814

https://nvd.nist.gov/vuln/detail/CVE-2025-5365	7,3	Campcodes Online Hospital Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/yuanchaoxxxxx/CVE/issues/1 https://vuldb.com/?ctiid.310659 https://vuldb.com/?id.310659 https://vuldb.com/?submit.586700 https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-37089	7,2	HPE StoreOnce Software	Improper Neutralization of Special Elements used in a Command ('Command Injection')		https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04847en_us&docLocale=en_US

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Five Known Exploited Vulnerabilities to Catalog	▪ CVE-2021-32030 ASUS Routers Improper Authentication Vulnerability ▪ CVE-2023-39780 ASUS RT-AX55 Routers OS Command Injection Vulnerability ▪ CVE-2024-56145 Craft CMS Code Injection Vulnerability ▪ CVE-2025-3935 ConnectWise ScreenConnect Improper Authentication Vulnerability ▪ CVE-2025-35939 Craft CMS External Control of Assumed-Immutable Web Parameter Vulnerability	https://www.cisa.gov/news-events/alerts/2025/06/02/cisa-adds-five-known-exploited-vulnerabilities-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
Week in review: NIST proposes new vulnerabilities metric, flaws in NASA's open source software	https://www.helpnetsecurity.com/2025/06/01/week-in-review-nist-proposes-new-vulnerabilities-metric-flaws-in-nasas-open-source-software/
Microsoft and CrowdStrike Launch Shared Threat Actor Glossary to Cut Attribution Confusion	https://thehackernews.com/2025/06/microsoft-and-crowdstrike-launch-shared.html
How One Path Traversal in Grafana Unleashed XSS, Open Redirect and SSRF (CVE-2025–4123)	https://infosecwriteups.com/how-one-path-traversal-in-grafana-unleashed-xss-open-redirect-and-ssrf-cve-2025-4123-b35245dccaab?source=collection_home

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Data Leak Exposes Details of Two Million Chinese Communist Party Members	https://www.infosecurity-magazine.com/news/data-leak-chinese-communist-party/
Cartier discloses data breach amid fashion brand cyberattacks	https://www.bleepingcomputer.com/news/security/cartier-discloses-data-breach-amid-fashion-brand-cyberattacks/
Next Step Healthcare data breach leaks patients' SSNs, medical records, and credit cards	https://www.comparitech.com/news/next-step-healthcare-data-breach-leaks-patients-ssns-medical-records-and-credit-cards/?&web_view=true

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Experts published a detailed analysis of Cisco IOS XE WLC flaw CVE-2025-20188	https://securityaffairs.com/178497/security/cisco-ios-xe-wlc-flaw-cve-2025-20188.html
Two flaws in vBulletin forum software are under attack	https://securityaffairs.com/178481/security/two-flaws-in-vbulletin-forum-software-are-under-attack.html
Linux Crash Reporting Flaws (CVE-2025-5054, 4598) Expose Password Hashes	https://hackread.com/linux-crash-reporting-flaws-expose-password-hashes/
New Chrome Zero-Day Actively Exploited; Google Issues Emergency Out-of-Band Patch	https://thehackernews.com/2025/06/new-chrome-zero-day-actively-exploited.html
New Linux Flaws Allow Password Hash Theft via Core Dumps in Ubuntu, RHEL, Fedora	https://thehackernews.com/2025/05/new-linux-flaws-allow-password-hash.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Sophos Firewall v21.5 is now available	https://news.sophos.com/en-us/2025/06/02/sophos-firewall-v21-5-is-now-available/
Qualcomm Fixes 3 Zero-Days Used in Targeted Android Attacks via Adreno GPU	https://thehackernews.com/2025/06/qualcomm-fixes-3-zero-days-used-in.html

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Backdoors in Python and NPM Packages Target Windows and Linux	https://hackread.com/backdoors-python-npm-packages-windows-linux/
Hackers Exploit AI Tools Misconfiguration To Run Malicious AI-generated Payloads	https://cybersecuritynews.com/hackers-exploit-ai-tools-misconfiguration/

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/