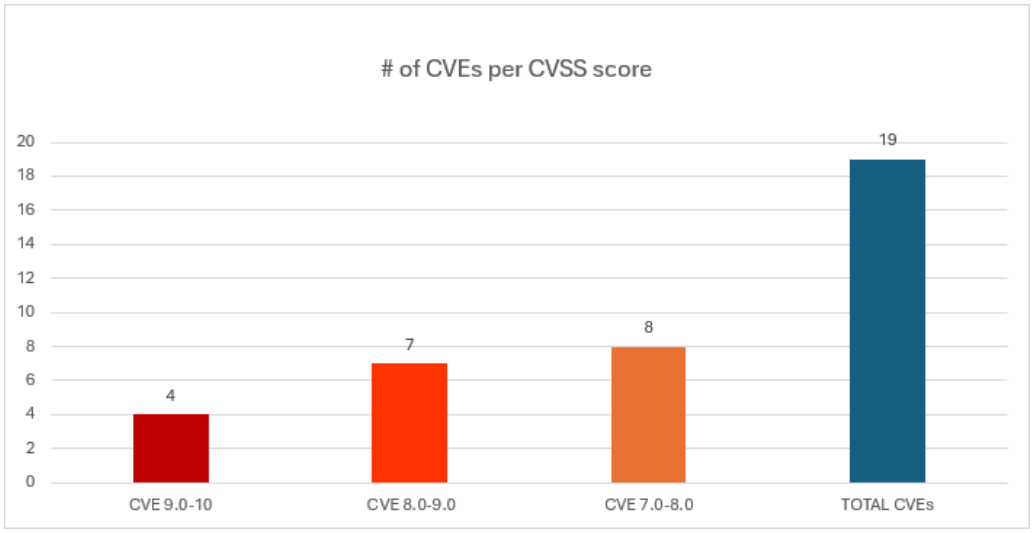
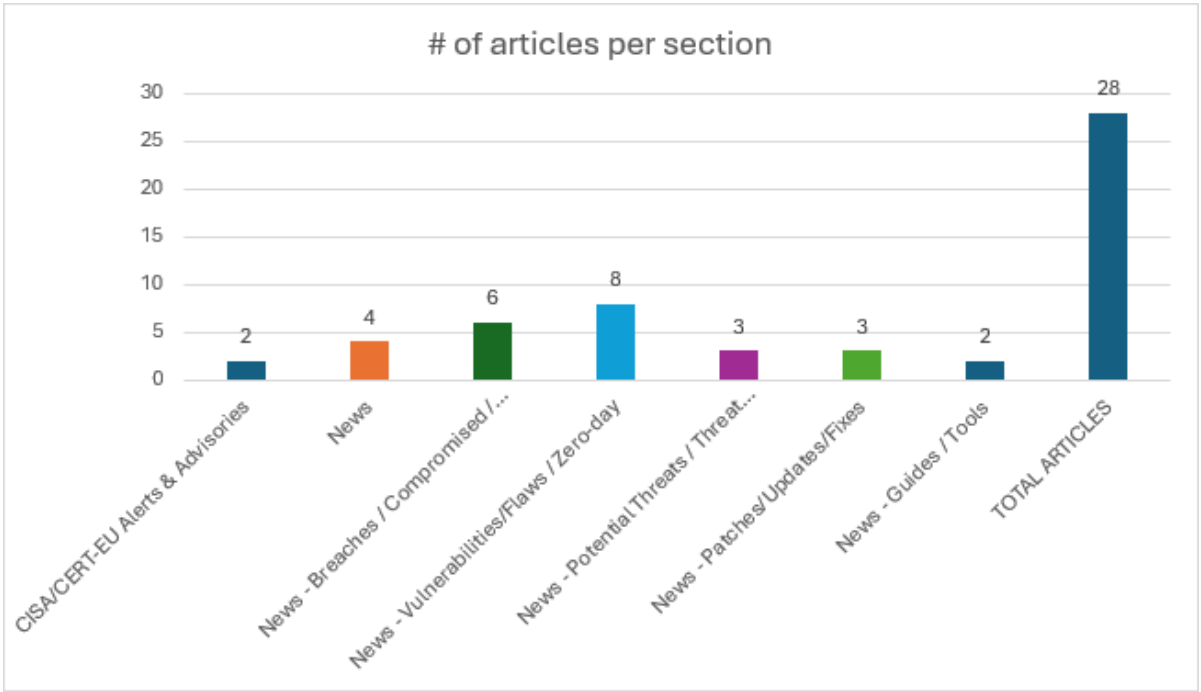
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 22/04/2025 - 25/04/2025





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-2025-31324	**10**	SAP NetWeaver Visual Composer Metadata Uploader	Unrestricted Upload of File with Dangerous Type		https://me.sap.com/notes/3594142 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2025-3604	**9,8**	The Flynax Bridge plugin for WordPress	Missing Authorization	all versions up to, and including, 2.2.0	https://plugins.trac.wordpress.org/browser/flynax-bridge/trunk/request.php https://www.wordfence.com/threat-intel/vulnerabilities/id/935caa43-4c75-47ad-a631-63988e21f834?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3603	**9,8**	The Flynax Bridge plugin for WordPress	Unverified Password Change	all versions up to, and including, 2.2.0	https://plugins.trac.wordpress.org/browser/flynax-bridge/trunk/request.php https://www.wordfence.com/threat-intel/vulnerabilities/id/fa8124db-ee6a-481d-88c6-4cc84fefcf1c?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-3065	**9,1**	The Database Toolset plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 1.8.4	https://plugins.trac.wordpress.org/browser/database-toolset/trunk/admin/class-database-toolset-admin.php#L109 https://wordpress.org/plugins/database-toolset/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0e656123-cae4-4e0c-a80a-98526be293a8?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3761	**8,8**	The My Tickets – Accessible Event Ticketing plugin for WordPress	Improper Privilege Management	all versions up to, and including, 2.0.16.	https://plugins.trac.wordpress.org/changeset/3280248/my-tickets/trunk/my-tickets.php https://www.wordfence.com/threat-intel/vulnerabilities/id/6d875c23-3d8a-4f82-bea3-1c46b5045d94?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3607	**8,8**	The Frontend Login and Registration Blocks plugin for WordPress	Unverified Password Change	all versions up to, and including, 1.0.7	https://plugins.trac.wordpress.org/browser/frontend-login-and-registration-blocks/trunk/inc/class-flr-blocks-lost-password.php#L115 https://www.wordfence.com/threat-intel/vulnerabilities/id/b06ce1e4-5cfb-415d-ad09-db194d6b4354?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3101	**8,8**	The Configurator Theme Core plugin for WordPress	Improper Privilege Management	all versions up to, and including, 1.4.7	https://themeforest.net/item/configurator-woocommerce-wordpress-theme/20474230 https://www.wordfence.com/threat-intel/vulnerabilities/id/535aa061-479f-415e-bee6-3151c42b917e?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-3058	**8,8**	The Xelion Webchat plugin for Word-Press	Missing Authorization	all versions up to, and including, 9.1.0	ttps://plugins.trac.wordpress.org/browser/xelion-web-chat/trunk//includes/class-xelion-webchat-ajax-ad-min.php#L119 https://www.wordfence.com/threat-intel/vulnerabili-ties/id/250202d5-3a0d-494c-8386-1f4cd015ad7e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3776]	**8,3**	The Verification SMS with TargetSMS plugin for Word-Press	Improper Control of Generation of Code ('Code Injection')	all versions up to, and including, 1.5	https://plugins.trac.wordpress.org/browser/verification-sms-targetsms/trunk/inc/ajax.php#L7 https://plugins.trac.wordpress.org/browser/verification-sms-targetsms/trunk/inc/ajax.php#L9 https://www.wordfence.com/threat-intel/vulnerabili-ties/id/ed08d248-7467-4a3b-91a2-4286d91b9c50?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3529	**8,2**	WordPress Simple Shopping Cart	Insertion of Sensitive Information Into Sent Data	all versions up to, and including, 5.1.2 via the 'file_url' pa-rameter	https://plugins.trac.wordpress.org/browser/wordpress-sim-ple-paypal-shopping-cart/tags/5.1.2/includes/wpsc-shortcodes-related.php#L92 https://plugins.trac.wordpress.org/changeset/3275373/ https://wordpress.org/plugins/wordpress-simple-paypal-shopping-cart/#developers https://www.tipsandtricks-hq.com/ecommerce/wp-simple-cart-sell-digital-downloads-2468 https://www.wordfence.com/threat-intel/vulnerabili-ties/id/8fecc015-518f-4aab-a17e-17cf4b8cf123?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2021-47663	**8,1**	JSON Web Tokens	Insufficient Session Expiration		https://www.sciencedirect.com/science/article/pii/S2351978921001657

https://nvd.nist.gov/vuln/detail/CVE-2025-3530	**7,5**	WordPress Simple Shopping Cart	External Control of Assumed-Immutable Web Parameter	all versions up to, and including, 5.1.2	https://plugins.trac.wordpress.org/browser/wordpress-simple-paypal-shopping-cart/tags/5.1.2/wp_shopping_cart.php#L156 https://plugins.trac.wordpress.org/browser/wordpress-simple-paypal-shopping-cart/tags/5.1.2/wp_shopping_cart.php#L165 https://plugins.trac.wordpress.org/browser/wordpress-simple-paypal-shopping-cart/tags/5.1.2/wp_shopping_cart.php#L171 https://plugins.trac.wordpress.org/browser/wordpress-simple-paypal-shopping-cart/tags/5.1.2/wp_shopping_cart.php#L261 https://plugins.trac.wordpress.org/changeset/3275373/ https://www.tipsandtricks-hq.com/wordpress-simple-paypal-shopping-cart-plugin-768 https://www.wordfence.com/threat-intel/vulnerabilities/id/e0a3910b-adc4-4633-a6a1-32ba50894be4?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2021-47662	**7,5**	HTTPS	Missing Authorization		https://www.sciencedirect.com/science/article/pii/S2351978921001657

https://nvd.nist.gov/vuln/detail/CVE-2025-3300	**7,2**	The WPMaster-ToolKit (WPMTK) – All in one plugin plugin for Word-Press	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 2.5.2	https://wordpress.org/plugins/wpmastertoolkit/ https://www.wordfence.com/threat-intel/vulnerabili-ties/id/c389ba1a-45c5-4fba-9b99-0713fe39da42?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-1294	**7,2**	The eForm - Word-Press Form Builder plugin for Word-Press	Improper Neutraliza-tion of Input During Web Page Generation ('Cross-site Scripting')	all versions up to, and including, 4.18.0	https://codecanyon.net/item/eform-wordpress-form-builder/3180835 https://eform.live/changelog/ https://www.wordfence.com/threat-intel/vulnerabili-ties/id/6c5db375-e865-47ba-a3dd-462c55d066fd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-46400	**7,1**	fig2dev	NULL Pointer Dereference	version 3.2.9a	https://sourceforge.net/p/mcj/tickets/187/
https://nvd.nist.gov/vuln/detail/CVE-2025-46399	**7,1**	fig2dev	NULL Pointer Dereference	version 3.2.9a	https://sourceforge.net/p/mcj/tickets/187/

https://nvd.nist.gov/vuln/detail/CVE-2025-46398	**7,1**	fig2dev	Stack-based Buffer Overflow	version 3.2.9a	https://sourceforge.net/p/mcj/tickets/191/
https://nvd.nist.gov/vuln/detail/CVE-2025-46397	**7,1**	fig2dev	Stack-based Buffer Overflow	version 3.2.9a	https://sourceforge.net/p/mcj/tickets/191/

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Five Industrial Control Systems Advisories	▪ ICSA-25-112-01 Siemens TeleControl Server Basic SQL ▪ ICSA-25-112-02 Siemens TeleControl Server Basic ▪ ICSA-25-112-03 Schneider Electric Wiser Home Controller WHC-5918A ▪ ICSA-25-112-04 ABB MV Drives	https://www.cisa.gov/news-events/alerts/2025/04/22/cisa-releases-five-industrial-control-systems-advisories
CISA Releases Seven Industrial Control Systems Advisories	▪ ICSA-25-114-01 Schneider Electric Modicon Controllers ▪ ICSA-25-114-02 ALBEDO Telecom Net.Time - PTP/NTP Clock ▪ ICSA-25-114-03 Vestel AC Charger ▪ ICSA-25-114-04 Nice Linear eMerge E3 ▪ ICSA-25-114-05 Johnson Controls ICU ▪ ICSA-25-114-06 Planet Technology Network Products ▪ ICSA-24-338-05 Fuji Electric Monitouch V-SFT (Update A)	https://www.cisa.gov/news-events/alerts/2025/04/24/cisa-releases-seven-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
Automating Zero Trust in Healthcare: From Risk Scoring to Dynamic Policy Enforcement Without Network Redesign	https://thehackernews.com/2025/04/automating-zero-trust-in-healthcare.html
WhatsApp's New Advanced Chat Privacy Feature to Protect Sensitive Conversations	https://cybersecuritynews.com/whatsapp-advanced-chat-privacy-feature/
How Script-based Malware Attacks Work: Modern Examples	https://cybersecuritynews.com/how-script-based-malware-attacks-work-modern-examples/
Hackers Weaponized Google Forms to Evade Email Security & Steal Logins	https://cybersecuritynews.com/google-forms-weaponized/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Lazarus hackers breach six companies in watering hole attacks	https://www.bleepingcomputer.com/news/security/lazarus-hackers-breach-six-companies-in-watering-hole-attacks/
Frederick Health data breach impacts nearly 1 million patients	https://www.bleepingcomputer.com/news/security/frederick-health-data-breach-impacts-nearly-1-million-patients/
Yale New Haven Health (YNHHS) data breach impacted 5.5 million patients	https://securityaffairs.com/176937/data-breach/yale-new-haven-health-ynhhs-data-breach-impacted-5-5-million-patients.html
Data breach victimization in the US escalates	https://scmagazine.com/brief/data-breach-victimization-in-the-us-escalates
Blue Shield Leaked Millions of Patient Info to Google for Years	https://hackread.com/blue-shield-leaked-millions-patient-info-google-years/
Interlock ransomware claims DaVita attack, leaks stolen data	https://www.bleepingcomputer.com/news/security/interlock-ransomware-claims-davita-attack-leaks-stolen-data/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Microsoft now pays up to $30,000 for some AI vulnerabilities	https://www.bleepingcomputer.com/news/microsoft/microsoft-now-pays-up-to-30-000-for-some-ai-vulnerabilities/
Microsoft's Symlink Patch Created New Windows DoS Vulnerability	https://cybersecuritynews.com/microsofts-symlink-patch-dos-vulnerability/
Vulnerability Exploitation and Credential Theft Now Top Initial Access Vectors	https://www.infosecurity-magazine.com/news/vulnerability-credential-initial/
Cisco Confirms Multiple Products Impacted by Erlang/OTP SSH Server RCE Vulnerability	https://cybersecuritynews.com/cisco-confirms-multiple-products-impacted/
SAP NetWeaver 0-day Vulnerability Exploited in the Wild to Deploy Webshells	https://cybersecuritynews.com/sap-netweaver-0-day-vulnerability/
Linux io_uring Security Blind Spot Let Attackers Stealthily Deploy Rootkits	https://cybersecuritynews.com/linux-io_uring-security-blind-spot/
Critical Vulnerabilities in Browser Wallets Let Attackers Drain your Funds	https://cybersecuritynews.com/critical-browser-wallet-vulnerabilities/
NVIDIA NeMo Framework Vulnerability Let Attackers Execute Remote Code	https://cybersecuritynews.com/nvidia-nemo-framework-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Microsoft fixes machine learning bug flagging Adobe emails as spam	https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-machine-learning-bug-flagging-adobe-emails-as-spam/
Commvault Command Center bug rated 10.0 patched	https://scmagazine.com/news/commvault-command-center-bug-rated-100-patched
GitLab Security Update – Patch for XSS, DoS & Account Takeover Vulnerabilities	https://cybersecuritynews.com/gitlab-security-update/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Hackers abuse OAuth 2.0 workflows to hijack Microsoft 365 accounts	https://www.bleepingcomputer.com/news/security/hackers-abuse-oauth-20-workflows-to-hijack-microsoft-365-accounts/
ELENOR-corp Ransomware Targets Healthcare Sector	https://www.infosecurity-magazine.com/news/elenor-corp-ransomware-targets/
Threat Actors Attacking Organization in Thailand to Deploy Ransomware	https://cybersecuritynews.com/threat-actors-attacking-organization-in-thailand/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best Cyber Attack Simulation Tools – 2025	**https://cybersecuritynews.com/cyber-attack-simulation-tools/**
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/