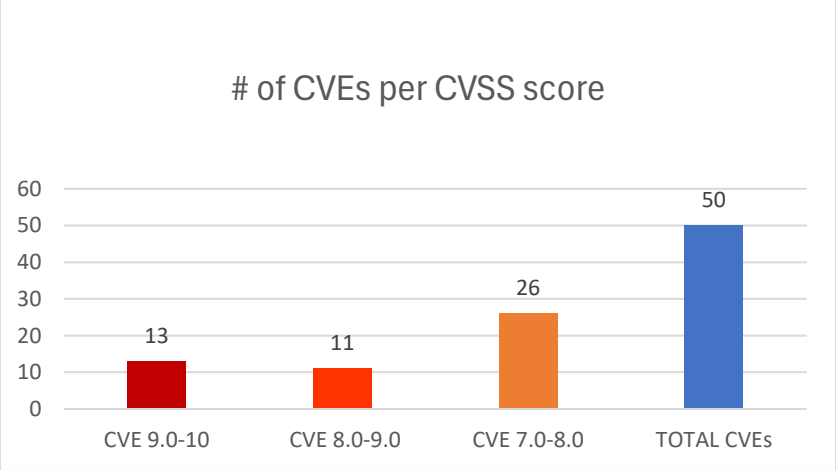
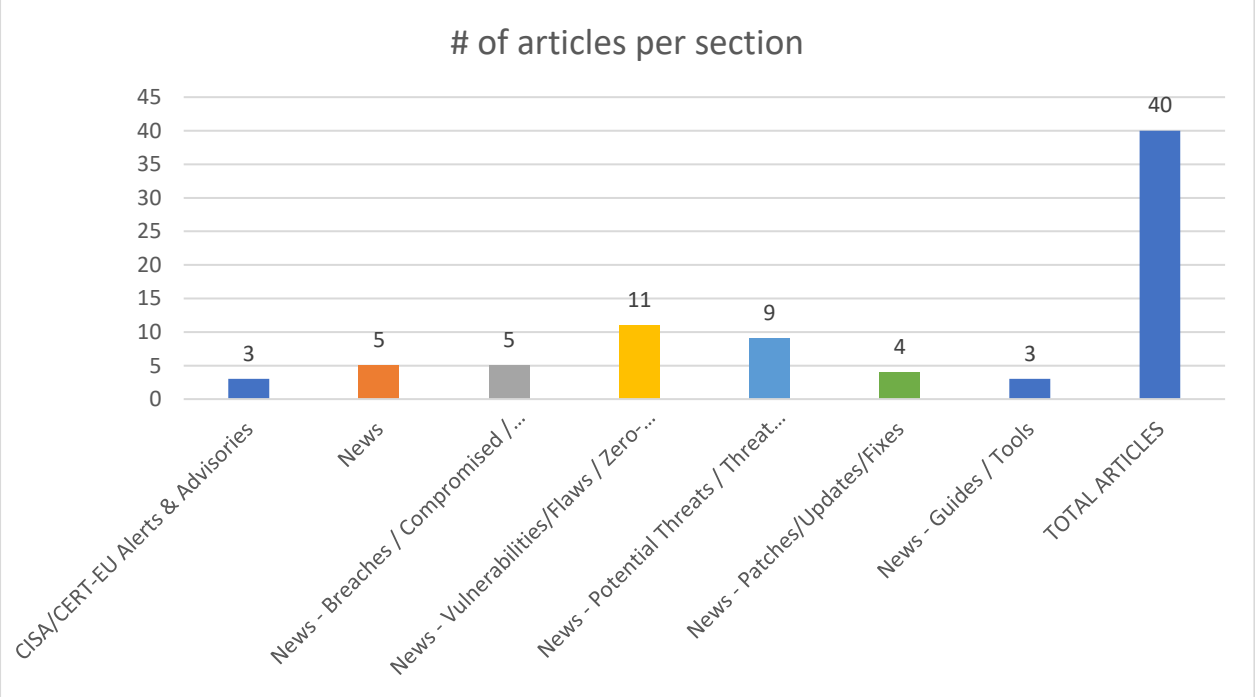
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 20/08/2025 - 22/08/2025





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-2025-53577	10,0	Global DNS	Improper Control of Generation of Code ('Code Injection')	from n/a through 3.1.0	https://patchstack.com/database/wordpress/plugin/global-dns/vulnerability/wordpress-global-dns-plugin-3-1-0-remote-code-execution-rce-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-48169	9,9	Jordy Meow Code Engine	Improper Control of Generation of Code ('Code Injection')	from n/a through 0.3.3	https://patchstack.com/database/wordpress/plugin/code-engine/vulnerability/wordpress-code-engine-plugin-0-3-3-remote-code-execution-rce-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53213	9,9	ELEXtensions ReachShip WooCommerce Multi-Carrier & Conditional Shipping	Unrestricted Upload of File with Dangerous Type	from n/a through 4.3.1	https://patchstack.com/database/wordpress/plugin/elex-reachship-multi-carrier-conditional-shipping/vulnerability/wordpress-reachship-woocommerce-multi-carrier-conditional-shipping-4-3-1-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54049	9,9	Custom API for WP	Incorrect Privilege Assignment	from n/a through 4.2.2	https://patchstack.com/database/wordpress/plugin/custom-api-for-wp/vulnerability/wordpress-custom-api-for-wp-4-2-2-privilege-escalation-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53299	9,8	ThemeMakers Visual Content Composer	Deserialization of Untrusted Data	from n/a through 1.5.8	https://patchstack.com/database/wordpress/plugin/tmm_content_composer/vulnerability/wordpress-thememakers-visual-content-composer-plugin-1-5-8-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53580	9,8	Simple Business Directory Pro	Incorrect Privilege Assignment	from n/a through n/a	https://patchstack.com/database/wordpress/plugin/simple-business-directory-pro/vulnerability/wordpress-simple-business-directory-pro-plugin-15-6-9-privilege-escalation-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-54014	9,8	MediCenter - Health Medical Clinic	Deserialization of Untrusted Data	from n/a through 15.1	https://patchstack.com/database/wordpress/theme/medicenter/vulnerability/wordpress-medicenter-health-medical-clinic-15-1-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54713	9,8	Taxi Booking Manager for WooCommerce	Authentication Bypass Using an Alternate Path or Channel	from n/a through 1.3.0	https://patchstack.com/database/wordpress/plugin/ecab-taxi-booking-manager/vulnerability/wordpress-taxi-booking-manager-for-woocommerce-plugin-1-3-0-broken-authentication-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-49381	9,6	ads.txt Guru	Cross-Site Request Forgery (CSRF)	from n/a through 1.1.1	https://patchstack.com/database/wordpress/plugin/adstxt-guru-connect/vulnerability/wordpress-ads-txt-guru-connect-plugin-1-1-1-cross-site-request-forgery-csrf-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54726	9,3	JS Archive List	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through n/a	https://patchstack.com/database/wordpress/plugin/jquery-archive-list-widget/vulnerability/wordpress-js-archive-list-plugin-6-1-6-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9288	9,1	sha.js	Improper Input Validation	through 2.4.11	https://github.com/browserify/sha.js/pull/78 harborist https://github.com/browserify/sha.js/security/advisories/GHSA-95m3-7q98-8xr5 harborist https://www.cve.org/CVERecord?id=CVE-2025-9287
https://nvd.nist.gov/vuln/detail/CVE-2025-9287	9,1	cipher-base	Improper Input Validation	through 1.0.4	https://github.com/browserify/cipher-base/pull/23 harborist https://github.com/browserify/cipher-base/security/advisories/GHSA-cpq7-6gpm-g9rc
https://nvd.nist.gov/vuln/detail/CVE-2025-54677	9,1	Online Booking & Scheduling Calendar for WordPress by vcita	Unrestricted Upload of File with Dangerous Type	from n/a through 4.5.3	https://patchstack.com/database/wordpress/plugin/meeting-scheduler-by-vcita/vulnerability/wordpress-online-booking-scheduling-calendar-for-wordpress-by-vcita-plugin-4-5-3-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-48165	8,8	DELUCKS DELUCKS SEO	Incorrect Privilege Assignment	from n/a through 2.6.0	https://patchstack.com/database/wordpress/plugin/delucks-seo/vulnerability/wordpress-delucks-seo-plugin-2-6-0-privilege-escalation-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-49382	8,8	DexignZone JobZilla - Job Board Word-Press Theme	Cross-Site Request Forgery (CSRF)	from n/a through 2.0	https://patchstack.com/database/wordpress/theme/jobzilla/vulnerability/wordpress-jobzilla-job-board-wordpress-theme-theme-2-0-cross-site-request-forgery-csrf-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-49399	8,8	Basix NEX-Forms	Cross-Site Request Forgery (CSRF)	from n/a through 9.1.3	https://patchstack.com/database/wordpress/plugin/nex-forms-express-wp-form-builder/vulnerability/wordpress-nex-forms-plugin-9-1-3-cross-site-request-forgery-csrf-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53560	8,8	Noisa	Deserialization of Untrusted Data	from n/a through 2.6.0	https://patchstack.com/database/wordpress/theme/noisa/vulnerability/wordpress-noisa-2-6-0-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54735	8,8	CubeWP Framework	Incorrect Privilege Assignment	from n/a through 1.1.24	https://patchstack.com/database/wordpress/plugin/cubewp-framework/vulnerability/wordpress-cubewp-framework-plugin-1-1-24-privilege-escalation-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53194	8,5	Crocoblock JetEngine	Improper Neutralization of Special Elements Used in a Template En-gine	from n/a through 3.7.0	https://patchstack.com/database/wordpress/plugin/jet-engine/vulnerability/wordpress-jetengine-3-7-0-remote-code-execution-rce-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-48171	8,1	Cena Store	Improper Control of Filename for Include/Require State-ment in PHP Program ('PHP Remote File Inclusion	from n/a through 2.11.26	https://patchstack.com/database/wordpress/theme/cena/vulnerability/wordpress-cena-store-2-11-26-local-file-inclusion-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-53207	8,1	WP Travel Gutenberg Blocks	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 3.9.0	https://patchstack.com/database/wordpress/plugin/wp-travel-blocks/vulnerability/wordpress-wp-travel-gutenberg-blocks-3-9-0-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53198	8,1	Houzez	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 4.0.4	https://patchstack.com/database/wordpress/theme/houzez/vulnerability/wordpress-houzez-4-0-4-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53565	8,1	Widget for Google Reviews	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 1.0.15	https://patchstack.com/database/wordpress/plugin/business-reviews-wp/vulnerability/wordpress-widget-for-google-reviews-1-0-15-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53567	8,1	Ghost Kit	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 3.4.1	https://patchstack.com/database/wordpress/plugin/ghostkit/vulnerability/wordpress-ghost-kit-3-4-1-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-48298	7,5	Benjamin Denis SEOPress for MainWP	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 1.4	https://patchstack.com/database/wordpress/plugin/seopress-for-mainwp/vulnerability/wordpress-seopress-for-mainwp-1-4-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-48302	7,5	Roxnor FundEngine	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusio	from n/a through 1.7.4	https://patchstack.com/database/wordpress/plugin/wp-fundraising-donation/vulnerability/wordpress-fundengine-plugin-1-7-4-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53210	7,5	ZoloBlocks	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 2.3.2	https://patchstack.com/database/wordpress/plugin/zoloblocks/vulnerability/wordpress-zoloblocks-plugin-2-3-2-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/	7,5	Maya Business	Authorization Bypass Through User-Controlled Key	from n/a through 1.2.0	https://patchstack.com/database/wordpress/plugin/paymaya-checkout-for-woocommerce/vulnerability/wordpress-maya-

CVE-2025-53208					business-1-2-0-insecure-direct-object-references-idor-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54017	7,5	Paid Member Subscriptions	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 2.15.4	https://patchstack.com/database/wordpress/plugin/paid-member-subscriptions/vulnerability/wordpress-paid-member-subscriptions-2-15-4-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54021	7,5	Mitchell Bennis Simple File List	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	from n/a through 6.1.14	https://patchstack.com/database/wordpress/plugin/simple-file-list/vulnerability/wordpress-simple-file-list-6-1-14-arbitrary-file-download-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54028	7,5	CF7 WOW Styler	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 1.7.2	https://patchstack.com/database/wordpress/plugin/cf7-styler/vulnerability/wordpress-cf7-wow-styler-plugin-1-7-2-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54052	7,5	Realtyna Realtyna Organic IDX plugin	Cross-Site Request Forgery (CSRF)	from n/a through 5.0.0	https://patchstack.com/database/wordpress/plugin/real-estate-listing-realtyna-wpl/vulnerability/wordpress-realtyna-organic-idx-plugin-plugin-5-0-0-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54034	7,5	Newsletters	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 4.10	https://patchstack.com/database/wordpress/plugin/newsletters-lite/vulnerability/wordpress-newsletters-4-10-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-57732	7,5	JetBrains TeamCity	Improper Ownership Management	before 2025.07.1	https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2025-9253	7,4	Linksys	Stack-based Buffer Overflow	RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/	https://github.com/wudipjq/my_vuln/blob/main/Linksys/vuln_17/17.md VulDB https://vuldb.com/?ctiid.320779 VulDB https://vuldb.com/?id.320779 VulDB https://vuldb.com/?submit.631521 VulDB https://www.linksys.com/

				1.0.04.002/1.1.05.003/1.2.07.001	
https://nvd.nist.gov/vuln/detail/CVE-2025-49438	7,2	Max Chirkov Simple Login Log	Deserialization of Untrusted Data	from n/a through 1.1.3	https://patchstack.com/database/wordpress/plugin/simple-login-log/vulnerability/wordpress-simple-login-log-plugin-1-1-3-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54012	7,2	Welcart e-Commerce	Deserialization of Untrusted Data	from n/a through 2.11.16	https://patchstack.com/database/wordpress/plugin/usc-e-shop/vulnerability/wordpress-welcart-e-commerce-plugin-2-11-16-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-48170	7,1	LambertGroup Universal Video Player - Addon for WPBakery	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 3.2.1	https://patchstack.com/database/wordpress/plugin/lbg-universal-video-player-addon-visual-composer/vulnerability/wordpress-universal-video-player-addon-for-wpbakery-page-builder-3-2-1-cross-site-scripting-xss-vulnerability-2?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-48296	7,1	skygroup UpStore	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 1.7.0	https://patchstack.com/database/wordpress/theme/upstore/vulnerability/wordpress-upstore-1-7-0-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-48297	7,1	quantumcloud Simple Link Directory	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through n/a	https://patchstack.com/database/wordpress/plugin/qc-simple-link-directory/vulnerability/wordpress-simple-link-directory-14-8-1-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53226	7,1	Comments Capcha Box	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 1.1	https://patchstack.com/database/wordpress/plugin/comments-capcha-box/vulnerability/wordpress-comments-capcha-box-plugin-1-1-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53212	7,1	LambertGroup Revolution Video Player	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 2.9.2	https://patchstack.com/database/wordpress/plugin/revolution-video-player/vulnerability/wordpress-revolution-video-player-with-bottom-playlist-2-9-2-cross-site-scripting-xss-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-53205	7,1	Radio Player Shoutcast & Icecast	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 4.4.7	https://patchstack.com/database/wordpress/plugin/lbg-audio4-html5-shoutcast/vulnerability/wordpress-radio-player-shoutcast-icecast-4-4-7-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53201	7,1	NooTheme Jobmonster	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 4.7.8	https://patchstack.com/database/wordpress/theme/noo-jobmonster/vulnerability/wordpress-jobmonster-4-7-8-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53319	7,1	Raptive Ads	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 3.8.0	https://patchstack.com/database/wordpress/plugin/adthrive-ads/vulnerability/wordpress-raptive-ads-plugin-3-8-0-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53563	7,1	LambertGroup Youtube Vimeo Video Player and Slider	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 3.8	https://patchstack.com/database/wordpress/plugin/video_player_youtube_vimeo/vulnerability/wordpress-youtube-vimeo-video-player-and-slider-3-8-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54027	7,1	Support Board	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 3.8.0	https://patchstack.com/database/wordpress/plugin/supportboard/vulnerability/wordpress-support-board-3-8-0-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54056	7,1	Responsive HTML5 Audio Player PRO With Playlist	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 3.5.8	https://patchstack.com/database/wordpress/plugin/lbg-audio2-html5/vulnerability/wordpress-responsive-html5-audio-player-pro-with-playlist-3-5-8-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54044	7,1	Elite Video Player	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 10.0.5	https://patchstack.com/database/wordpress/plugin/elite-video-player/vulnerability/wordpress-elite-video-player-10-0-5-cross-site-scripting-xss-vulnerability-2?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54032	7,1	Real Estate Manager Pro	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through 12.7.3	https://patchstack.com/database/wordpress/plugin/real-estate-manager-pro/vulnerability/wordpress-real-estate-manager-pro-plugin-12-7-3-cross-site-scripting-xss-vulnerability?_s_id=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Four ICS Advisories Surrounding Vulnerabilities, and Exploits		**https://cybersecuritynews.com/cisa-releases-four-ics-advisories/**
CISA Adds One Known Exploited Vulnerability to Catalog	▪ **CVE-2025-43300 Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability**	https://www.cisa.gov/news-events/alerts/2025/08/21/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Three Industrial Control Systems Advisories	▪ **ICSA-25-233-01 Mitsubishi Electric Corporation MELSEC iQ-F Series CPU Module** ▪ **ICSA-25-177-01 Mitsubishi Electric Air Conditioning Systems (Update A)** ▪ **ICSMA-25-233-01 FUJIFILM Healthcare Americas Synapse Mobility**	https://www.cisa.gov/news-events/alerts/2025/08/21/cisa-releases-three-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
Whitepaper: The evolution of phishing attacks	**https://pushsecurity.com/resources/phishing-evolution?utm_campaign=18916228-FY25Q3_Phishing-evolution-white-paper&utm_source=bleepingcomputer&utm_content=whitepaper**
FBI Warns FSB-Linked Hackers Exploiting Unpatched Cisco Devices for Cyber Espionage	https://thehackernews.com/2025/08/fbi-warns-russian-fsb-linked-hackers.html
ISACA Launches AI-Centric Security Management Certification	**https://www.infosecurity-magazine.com/news/isaca-aicentric-security/**
Easy ChatGPT Downgrade Attack Undermines GPT-5 Security	https://www.darkreading.com/application-security/chatgpt-downgrade-attack-gpt-5-security
NIST Unveils Guidelines to Help Spot Face Morphing Attempts	**https://www.infosecurity-magazine.com/news/nist-unveils-guidelines-spot-face/**

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Intel Employee Data Exposed by Vulnerabilities	**https://www.securityweek.com/intel-employee-data-exposed-by-vulnerabilities/**
Pharmaceutical Company Inotiv Confirms Ransomware Attack	https://www.infosecurity-magazine.com/news/pharma-inotiv-confirms-ransomware/
NY Business Council discloses data breach affecting 47,000 people	https://www.bleepingcomputer.com/news/security/business-council-of-new-york-state-discloses-data-breach-affecting-47-000-people/?&web_view=true
New MITM6 + NTLM Relay Attack Let Attackers Escalate Privileges and Compromise Entire Domain	**https://cybersecuritynews.com/new-mitm6-ntlm-relay-attack/**
Qilin Ransomware Gang Claims 4TB Data Breach at Nissan CBI	https://hackread.com/qilin-ransomware-gang-4tb-data-breach-nissan-cbi/?&web_view=true

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Warlock Ransomware Hitting Victims Globally Through SharePoint ToolShell Exploit	https://www.infosecurity-magazine.com/news/warlock-ransomware-sharepoint/
Critical Apache Tika PDF Parser Vulnerability Allow Attackers to Access Sensitive Data	https://cybersecuritynews.com/apache-tika-pdf-parser-vulnerability/
Hackers Exploiting Apache ActiveMQ Flaw to Infiltrate Cloud-Based Linux Systems	https://cybersecuritynews.com/apache-activemq-vulnerability-exploited/
Lenovo AI Chatbot Vulnerability Let Attackers Run Remote Scripts on Corporate Machines	https://cybersecuritynews.com/lenovo-ai-chatbot-vulnerability/
Paper Werewolf Exploiting WinRAR Zero-Day Vulnerability to Deliver Malware	https://cybersecuritynews.com/paper-werewolf-exploiting-winrar-zero%e2%80%91day/
Critical Namespace Injection Vulnerability in Kubernetes Capsule Let Attackers Inject Arbitrary Labels	https://cybersecuritynews.com/namespace-injection-in-kubernetes-capsule/
Copilot Vulnerability Breaks Audit Logs and Access Files Secretly for Hackers	https://cybersecuritynews.com/copilot-vulnerability-breaks-audit-logs/
Russian Hackers Exploiting 7-Year-Old Cisco Vulnerability to Collect Configs from Industrial Systems	https://cybersecuritynews.com/russian-hackers-exploiting-7-year-old-cisco-vulnerability/
Chrome High-Severity Vulnerability Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/chrome-high-severity-vulnerability/
CodeRabbit's Production Servers RCE Vulnerability Enables Write Access on 1M Repositories	https://cybersecuritynews.com/coderabbits-production-servers-rce-vulnerability/
Russian Espionage Group Static Tundra Targets Legacy Cisco Flaw	https://www.infosecurity-magazine.com/news/russian-espionage-group-targets/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Apple Patches CVE-2025-43300 Zero-Day in iOS, iPadOS, and macOS Exploited in Targeted Attacks	https://thehackernews.com/2025/08/apple-patches-cve-2025-43300-zero-day.html
Microsoft Issues Out-of-Band Update to Fix Recovery Issues	https://www.infosecurity-magazine.com/news/microsoft-outofband-update/
Microsoft Releases Emergency Updates to Fix Windows Reset and Recovery Error	https://cybersecuritynews.com/windows-reset-and-recovery-error-fix/
Vulnerabilities High-Severity Vulnerabilities Patched in Chrome, Firefox	https://www.securityweek.com/high-severity-vulnerabilities-patched-in-chrome-firefox/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
FBI Warns FSB-Linked Hackers Exploiting Unpatched Cisco Devices for Cyber Espionage	https://thehackernews.com/2025/08/fbi-warns-russian-fsb-linked-hackers.html
DOM-Based Extension Clickjacking Exposes Popular Password Managers to Credential and Data Theft	https://thehackernews.com/2025/08/dom-based-extension-clickjacking.html
Hackers Weaponize Active Directory Federation Services and office.com to Steal Microsoft 365 logins	https://cybersecuritynews.com/phishing-campaign-microsoft-365/
Elastic Refutes Claims of Zero-Day in EDR Product	https://www.securityweek.com/elastic-refutes-claims-of-zero-day-in-edr-product/
Threat Actors Leverage GenAI Platforms to Create Realistic Phishing Content	https://cybersecuritynews.com/threat-actors-leverage-genai-platforms/
Hackers Weaponize QR Codes in New 'Quishing' Attacks	https://www.infosecurity-magazine.com/news/hackers-qr-codes-new-quishing/
New SHAMOS Malware Attacking macOS Via Fake Help Websites to Steal Login Credentials	https://cybersecuritynews.com/new-shamos-malware-attacking-macos/
New Loader Malware Dubbed 'QuirkyLoader' Delivering Infostealers and RATs	https://cybersecuritynews.com/new-loader-malware-dubbed-quirkyloader/
DragonForce Ransomware Attack Analysis – Targets, TTPs and IoCs	https://cybersecuritynews.com/dragonforce-ransomware-attack/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/
10 Best Vulnerability Management Tools In 2025	https://cybersecuritynews.com/vulnerability-management-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-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.

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/