Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 14/03/2025 - 18/03/2025

Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 13
News 13
Breaches / Compromised / Hacked 13
Vulnerabilities / Flaws / Zero-day 14
Patches / Updates / Fixes 14
Potential threats / Threat intelligence 14
Guides / Tools 14
References 15
Annex – Websites with vendor specific vulnerabilities 16

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVS Sv3	Προϊόν/Υ-πηρεσία	Τύπος Ευπά-θειας	Συ-σκευές/Εκ δόσεις που επη-ρεάζονται	Συσκευές/Εκ-δόσεις που ΔΕΝ επηρεά-ζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-1771	**9,8**	Traveler theme for WordPress	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File In-clusion')	all versions up to, and including, 3.1.8	N/A	https://travelerwp.com/traveler-changelog/ https://www.wordfence.com/threat-intel/vulnerabilities/id/da3e3d6c-7643-4f22-aa88-2c4ce80aed1f?source=cve
https://github.com/advisories/GHSA-6m2c-76ff-6vrf	**9,8**	GitHub	Deserialization of Untrusted Data	N/A	Patches Fixed in Qiskit 1.4.2 and in Qiskit 2.0.0rc2	https://www.ibm.com/support/pages/node/7185949
https://nvd.nist.gov/vuln/detail/CVE-2025-2232	**9,8**	WordPress	Improper Privilege Management	The Real-teo - Real Estate Plugin by Pure-themes plugin for Word-Press. All versions up to, and including, 1.2.8	N/A	https://docs.purethemes.net/findeo/knowledge-base/changelog-findeo/ https://www.wordfence.com/threat-intel/vulnerabilities/id/abe73ecd-1325-4d6d-8545-d27f6116ca43?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2024-13771	**9,8**	WordPress	Authentication Bypass Using an Alternate Path or Channel	The Civi - Job Board & Freelance Marketplace WordPress Theme plugin for WordPress including, 2.1.4	N/A	http://localhost:1337/wp-content/themes/civi/includes/class-ajax.php#L715 https://www.wordfence.com/threat-intel/vulnerabilities/id/5ab2c74d-b83b-40ea-951c-83aeb76a7515?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-13824	**9,8**	WordPress	Deserialization of Untrusted Data	The CiyaShop - Multipurpose WooCommerce Theme theme for WordPress all versions up to, and including, 4.19.0	N/A	https://themeforest.net/item/ciyashop-responsive-multipurpose-woocommerce-wordpress-theme/22055376#item-description__changelog https://www.wordfence.com/threat-intel/vulnerabilities/id/b69c86f4-d81d-4e14-baff-3402008bb9c6?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-26875	**9,3**	Woocommerce	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through 1.3	N/A	https://patchstack.com/database/wordpress/plugin/different-shipping-and-billing-address-for-woocommerce/vulnerability/wordpress-multiple-shipping-and-billing-address-for-woocommerce-plugin-1-3-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-26921	**8,8**	Booking and Rental Manager	Deserialization of Untrusted Data	from n/a through 2.2.6	N/A	https://patchstack.com/database/wordpress/plugin/booking-and-rental-manager-for-woocommerce/vulnerability/wordpress-booking-and-rental-manager-plugin-2-2-6-php-object-injection-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-1667	**8,8**	The School Management System – WPSchoolPress plugin for WordPress	Authorization Bypass Through User-Controlled Key	all versions up to, and including, 2.2.16	N/A	https://plugins.trac.wordpress.org/browser/wpschoolpress/tags/2.2.16/lib/wpsp-ajaxworks-teacher.php#L544 https://www.wordfence.com/threat-intel/vulnerabilities/id/e54f98bc-c538-4f3c-b24a-6e778a3748ef?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-1657	**8,8**	The Directory Listings WordPress plugin	Missing Authorization	all versions up to, and including, 2.1.7	N/A	https://wordpress.org/plugins/ulisting/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0e70184f-94b6-4742-b99b-6eec9d28f17c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-1653	**8,8**	The Directory Listings WordPress plugin	Incorrect Privilege Assignment	all versions up to, and including, 2.1.7	N/A	https://wordpress.org/plugins/ulisting/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4181b26e-89c7-4020-a3d4-29bdc88d7438?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-46662	**8,8**	Fortinet	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Fortinet FortiManager versions 7.4.1 through 7.4.3, FortiManager Cloud versions 7.4.1 through 7.4.3	N/A	https://fortiguard.fortinet.com/psirt/FG-IR-24-222

https://nvd.nist.gov/vuln/detail/CVE-2024-13913	**8,8**	WordPress	Cross-Site Request Forgery (CSRF)	The InstaWP Connect – 1-click WP Staging & Migration plugin for WordPress. All versions up to, and including, 0.1.0.83	N/A	https://plugins.trac.wordpress.org/browser/instawp-connect/trunk/admin/class-instawp-admin.php#L159 https://plugins.trac.wordpress.org/browser/instawp-connect/trunk/migrate/templates/main.php#L27 https://plugins.trac.wordpress.org/changeset/3254817/ https://www.wordfence.com/threat-intel/vulnerabilities/id/ea6c7b63-00da-4476-a024-97fe99af643d?source=cve

https://github.com/advisories/GHSA-mrrh-fwg8-r2c3	**8,6**	GitHub	Embedded Malicious Code	tj-actions changed-files through 45.0.7	N/A	https://github.com/chains-project/maven-lockfile/pull/1111 https://github.com/espressif/arduino-esp32/issues/11127 https://github.com/github/docs/blob/962a1c8dccb8c0f66548b324e5b921b5e4fbc3d6/content/actions/security-for-github-actions/security-guides/security-hardening-for-github-actions.md?plain=1#L191-L193 https://github.com/modal-labs/modal-examples/issues/1100 https://github.com/rackerlabs/genestack/pull/903 https://github.com/tj-actions/changed-files/blob/45fb12d7a8bedb4da42342e52fe054c6c2c3fd73/README.md?plain=1#L20-L28 https://github.com/tj-actions/changed-files/issues/2463 https://github.com/tj-actions/changed-files/issues/2464 https://github.com/tj-actions/changed-files/issues/2477 https://news.ycombinator.com/item?id=43367987 https://news.ycombinator.com/item?id=43368870 https://semgrep.dev/blog/2025/popular-github-action-tj-actionschanged-files-is-compromised/ https://sysdig.com/blog/detecting-and-mitigating-the-tj-actions-changed-files-supply-chain-attack-cve-2025-30066/ https://web.archive.org/web/20250315060250/https://github.com/tj-actions/changed-files/issues/2463 https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised https://www.stream.security/post/github-action-supply-chain-attack-exposes-secrets-what-you-need-to-know-and-how-to-respond https://www.sweet.security/blog/cve-2025-30066-tj-actions-supply-chain-attack https://www.wiz.io/blog/github-action-tj-actions-changed-files-supply-chain-attack-cve-2025-30066
https://nvd.nist.gov/vuln/detail/CVE-2023-45588	**8,2**	FortiClientMac	External Control of File Name or Path	version 7.2.3 and below, version 7.0.10 and below	N/A	https://fortiguard.com/psirt/FG-IR-23-345

https://nvd.nist.gov/vuln/detail/CVE-2024-54027	**8,2**	FortiSandbox	Use of Hard-coded Cryptographic Key	version 4.4.6 and below, version 4.2.7 and below, version 4.0.5 and below, version 3.2.4 and below, version 3.1.5 and below, version 3.0.7 to 3.0.5	N/A	https://fortiguard.fortinet.com/psirt/FG-IR-24-327
https://nvd.nist.gov/vuln/detail/CVE-2025-30074	**7,8**	Alludo Parallels Desktop	Incorrect Authorization	Alludo Parallels Desktop before 19.4.2 and 20.x before 20.2.2 for macOS on Intel platforms	N/A	https://kb.parallels.com/en/130944
https://nvd.nist.gov/vuln/detail/CVE-2025-22473	**7,8**	Dell SmartFabric OS10 Software	Improper Neutralization of Special Elements used in a Command ('Command Injection')	version(s) 10.5.4.x, 10.5.5.x, 10.5.6.x, 10.6.0.x	N/A	https://www.dell.com/support/kbdoc/en-us/000289970/dsa-2025-070-security-update-for-dell-networking-os10-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000293638/dsa-2025-069-security-update-for-dell-networking-os10-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000294091/dsa-2025-079-security-update-for-dell-networking-os10-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000295014/dsa-2025-068-security-update-for-dell-networking-os10-vulnerabilities

https://nvd.nist.gov/vuln/detail/CVE-2025-30076	**7,7**	Koha	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Koha before 24.11.02	N/A	https://bugs.koha-community.org/bugzilla3/show_bug.cgi?id=39170 https://github.com/gl0wyy/koha-task-scheduler-rce
https://nvd.nist.gov/vuln/detail/CVE-2024-26006	**7,5**	FortiOS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	FortiOS version 7.4.3 and below, version 7.2.7 and below, version 7.0.13 and below and FortiProxy version 7.4.3 and below, version 7.2.9 and below, version 7.0.16 and below	N/A	https://fortiguard.fortinet.com/psirt/FG-IR-23-485
https://nvd.nist.gov/vuln/detail/CVE-2024-13321	**7,5**	WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	The AnalyticsWP plugin for WordPress all versions up to, and including, 2.0.0	N/A	https://analyticswp.com/ https://www.wordfence.com/threat-intel/vulnerabilities/id/f6507318-92c0-457c-8c87-2d023428a77f?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-2056	**7,5**	WordPress	Relative Path Traversal	The WP Ghost (Hide My WP Ghost) – Security & Firewall plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 5.4.01 via the showFile function	N/A	https://plugins.trac.wordpress.org/browser/hide-my-wp/tags/5.4.02/models/Files.php#L336 https://www.wordfence.com/threat-intel/vulnerabilities/id/f43db496-80ea-442c-9417-7aa03ec95f02?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-1764	**7,5**	WordPress	Cross-Site Request Forgery (CSRF)	The LoginPress | wp-login Custom Login Page Customizer plugin for WordPress all versions up to, and including, 3.3.1	N/A	https://plugins.svn.wordpress.org/loginpress/trunk/lib/wpb-sdk/views/wpb-debug.php https://plugins.trac.wordpress.org/changeset/3253283/ https://pt.wordpress.org/plugins/loginpress/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9df6a2b4-2dc4-43dd-8282-5c05b0fa13f6?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-2360	**7,3**	D-Link DIR-823G 1.0.2B05_20181207	Incorrect Privilege Assignment	This vulnerability only affects products that are no longer supported by the maintainer	Products that are supported by the maintainer	https://debricked.com/vulnerability-database/vulnerability/CVE-2025-2360 https://lavender-bicycle-a5a.notion.site/D-Link-DIR-823G-SetUpnpSettings-1ac53a41781f80d1a290c8d5da3e795e?pvs=4 https://vuldb.com/?ctiid.299827 https://vuldb.com/?id.299827 https://vuldb.com/?submit.513751 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-2322	**7,3**	springboot-openai-chatgpt	Use of Hard-coded Password	This affects an unknown part of the file /chatgpt-boot/src/main/java/org/springblade/modules/mjkj/controller/OpenController.java	N/A	https://vuldb.com/?ctiid.299751 https://vuldb.com/?id.299751 https://vuldb.com/?submit.505694 https://www.cnblogs.com/aibot/p/18732299
https://nvd.nist.gov/vuln/detail/CVE-2025-2320	**7,3**	springboot-openai-chatgpt	Incorrect Privilege Assignment	version details for affected and updated releases are not available	N/A	https://vuldb.com/?ctiid.299749 https://vuldb.com/?id.299749 https://vuldb.com/?submit.505689 https://www.cnblogs.com/aibot/p/18732226

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	**7,2**	WP Test Email plugin for Word-Press	Improper Neutral-ization of Input During Web Page Generation ('Cross-site Scripting')	all versions up to, and including, 1.1.8	N/A	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3251086%40wp-test-email&new=3251086%40wp-test-email&sfp_email=&sfph_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/7a0a9ff8-ed93-4de9-ba49-730b2253c6a4?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-13497	**7,2**	WordPress	Improper Neutral-ization of Script-Related HTML Tags in a Web Page (Basic XSS)	WordPress form builder plugin for contact forms, sur-veys and quizzes – Tripetto plugin for WordPress is vulnera-ble to Stored Cross-Site Scripting via attach-ment up-loads in all versions up to, and in-cluding, 8.0.9	N/A	https://plugins.trac.wordpress.org/browser/tripetto/trunk/lib/attachments.php#L46 https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3251202%40tripetto%2Ftrunk&old=3231968%40tripetto%2Ftrunk&sfp_email=&sfph_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/fbbe006c-1afc-4c8b-a9f3-ffb21cdabb54?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-26553	**7,1**	Spring Devs Pre Order Addon for WooCom-merce		This issue affects Pre Order Ad-don for WooCom-merce – Advance Or-der/Backor der Plugin: from n/a throu...	N/A	https://patchstack.com/database/wordpress/plugin/wc-pre-order/vulnerability/wordpress-pre-order-addon-for-woocommerce-plugin-1-0-7-reflected-cross-site-scripting?_s_id=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL

News

Σύντομη περιγραφή / Τίτλος	URL
Decrypting Linux/ESXi Akira Ransomware Files Without Paying Ransomware	https://cybersecuritynews.com/decrypting-linux-esxi-akira-ransomware-files/
CISA Releases Thirteen Industrial Control Systems Focusing Vulnerabilities & Exploits	https://cybersecuritynews.com/cisa-releases-thirteen-industrial-control-systems/
DeepSeek R1 Jailbreaked To Develop Malware, Such As A Keylogger And Ransomware	https://cybersecuritynews.com/deepseek-r1-jailbreaked/
Cybersecurity Weekly Recap: Key Updates on Attacks, Vulnerabilities, & Data Breaches	https://cybersecuritynews.com/cybersecurity-weekly-recap-2/
Hackers Exploit ChatGPT with CVE-2024-27564, 10,000+ Attacks in a Week	https://hackread.com/hackers-exploit-chatgpt-cve-2024-27564-10000-attacks/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
New Campaign Attacking PyPI Users to Steal Sensitive Data Including Cloud Tokens	https://cybersecuritynews.com/new-campaign-attacking-pypi-users/
Hackers Allegedly Selling 3.17 Million Records of Honda Cars India Customers	https://cybersecuritynews.com/hackers-allegedly-selling-honda-cars-data/
AWS SNS Abused To Exfiltrate Data & Phishing Attack	https://cybersecuritynews.com/aws-sns-abused/
Hackers Exploiting TP-Link Vulnerability to Gain Root Access	https://cybersecuritynews.com/hackers-exploiting-tp-link-vulnerability/
Hackers Exploiting CSS to Evade Spam Filters & Track User Actions	https://cybersecuritynews.com/hackers-exploiting-css-to-evade-spam-filters/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
SuperBlack Actors Exploiting Two Fortinet Vulnerabilities to Deploy Ransomware	https://cybersecuritynews.com/superblack-actors-exploiting-two-fortinet-vulnerabilities/
Lazarus Hackers Exploiting IIS Servers to Deploy ASP-based Web Shells	https://cybersecuritynews.com/lazarus-hackers-exploiting-iis-servers/
Critical ruby-saml Vulnerabilities Let Attackers Bypass Authentication	https://cybersecuritynews.com/ruby-saml-vulnerabilities-bypass-authentication/
Critical Vulnerabilities In Delphi Code Leads To Memory Corruption	https://cybersecuritynews.com/critical-vulnerabilities-in-delphi-code/
Adobe Acrobat Reader Vulnerabilities Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/adobe-acrobat-reader-vulnerabilities/
Vulnerability Summary for the Week of March 10, 2025	https://www.cisa.gov/news-events/bulletins/sb25-076

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Warns of Cyber Attack Mimic Booking .com To Deliver Password Stealing Malware	https://cybersecuritynews.com/microsoft-warns-of-cyber-attack-mimic-booking-com/
Cisco Warns of IOS XR Software Vulnerability That Let Attackers Trigger DoS condition	https://cybersecuritynews.com/cisco-warns-of-ios-xr-software-vulnerability/

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/