Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 11/03/2025 - 14/03/2025

Contents

1 Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv 3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	Συσκευές/Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-22954	10	Koha Library Software	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 24.11.02	N/A	https://koha-community.org/ https://bugs.koha-community.org/bugzilla3/show_bug.cgi?id=38829 https://koha-community.org/koha-24-11-02-released/
https://nvd.nist.gov/vuln/detail/CVE-2025-1960	9.8	Schneider Electric	Initialization of a Resource with an Insecure Default	N/A	N/A	https://www.se.com/ww/en/ https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-070-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-070-03.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-2263	9.8	Sante PACS Server	Stack-based Buffer Overflow	N/A	N/A	https://www.santesoft.com/win/sante-pacs-server/sante-pacs-server.html https://www.tenable.com/security/research/tra-2025-08
https://nvd.nist.gov/vuln/detail/CVE-2025-27407	9	GraphQL	Improper Control of Generation of Code ('Code Injection')	Starting in version 1.11.5 and prior to versions 1.11.8, 1.12.25, 1.13.24, 2.0.32, 2.1.14, 2.2.17, and 2.3.21	1.11.8, 1.12.25, 1.13.24, 2.0.32, 2.1.14, 2.2.17, and 2.3.21	https://graphql.org/ https://github.com/rmosolgo/graphql-ruby/security/advisories/GHSA-q92j-grw3-h492
https://nvd.nist.gov/vuln/detail/CVE-2025-2233	8.8	Samsung SmartThings	Improper Verification of Cryptographic Signature	N/A	N/A	https://www.samsung.com/gr/smartthings/ https://www.zerodayinitiative.com/advisories/ZDI-25-127/
https://nvd.nist.gov/vuln/detail/CVE-2025-1707	8.8	Review Schema plugin for WordPress	PHP Remote File Inclusion	all versions up to, and including, 2.2.4	N/A	https://wordpress.org/plugins/review-schema/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9b4de243-d337-4f29-a766-bcafb3848d1c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-25711	8.8	tNexus Airport View	Improper Preservation of Permissions	v.2.8	N/A	https://dtp.ae/tnexus-airport-view/ https://github.com/z5jt/vulnerability-research/tree/main/CVE-2025-25710
https://nvd.nist.gov/vuln/detail/CVE-2024-13913	8.8	InstaWP Connect – 1-click WP Staging &	Cross-Site Request Forgery (CSRF)	all versions up to, and including, 0.1.0.83	N/A	https://wordpress.org/plugins/instawp-connect/ https://www.wordfence.com/threat-

		Migration plugin for WordPress				intel/vulnerabilities/id/ea6c7b63-00da-4476-a024-97fe99af643d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-20146	8.6	Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers	Improper Input Validation	N/A	N/A	https://www.cisco.com/site/us/en/products/networking/software/ios-xr/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-multicast-ERMrSvq7
https://nvd.nist.gov/vuln/detail/CVE-2024-12858	7.8	Delta Electronics CNCSoft-G2	Heap-based Buffer Overflow	Version 2.1.0.16 and prior	N/A	https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=CNCSoft-g2&sort_expr=cdate&sort_dir=DESC https://filecenter.deltaww.com/news/download/doc/Delta-PCSA-2025-00002_CNCSoft-G2%20-%20Heap-based%20Buffer%20Overflow_v2.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-2271	7.7	Issuetrak	Authorization Bypass Through User-Controlled Key	v17.2.2 and prior	N/A	https://www.issuetrak.com/ https://helpcenter.issuetrak.com/home/2340-issuetrak-release-notes
https://nvd.nist.gov/vuln/detail/CVE-2024-26006	7.5	FortiOS & FortiProxy	Cross-site Scripting	version 7.4.3 and below, version 7.2.7 and below, version 7.0.13 and below version 7.4.3 and below, version 7.2.9 and below, version 7.0.16 and below	N/A	https://www.fortinet.com/products/fortigate/fortios https://fortiguard.fortinet.com/psirt/FG-IR-23-485
https://nvd.nist.gov/vuln/detail/CVE-2025-1764	7.5	LoginPress | wp-login Custom Login Page Customizer plugin for WordPress	Cross-Site Request Forgery (CSRF)	all versions up to, and including, 3.3.1	N/A	https://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-2024-10942	7.5	All-in-One WP Migration and Backup plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 7.89	N/A	https://wordpress.org/plugins/all-in-one-wp-migration/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0823d1d9-4f3b-4ac0-8cd1-ad208ebc325f?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-1119	7.3	Appointment Booking Calendar — Simply Schedule	Improper Control of Generation of Code ('Code Injection')	all versions up to, and including, 1.6.8.5	N/A	https://wordpress.org/plugins/simply-schedule-appointments/ https://www.wordfence.com/threat-

		Appointments Booking Plugin plugin for WordPress				intel/vulnerabilities/id/1be557db-daa8-4d86-819a-462f29da884b?source=cve

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Vulnerability Summary for the Week of March 3, 2025	Common Vulnerabilities and Exposures (CVE)	https://www.cisa.gov/news-events/bulletins/sb25-069
CISA Releases Industrial Control Systems Advisories	ICSA-25-070-01 Schneider Electric Uni-Telway Driver ICSA-25-070-02 Optigo Networks Visual BACnet Capture Tool/Optigo Visual Networks Capture Tool ICSA-25-072-01 Siemens Teamcenter Visualization and Tecnomatrix Plant Simulation ICSA-25-072-02 Siemens SINEMA Remote Connect Server ICSA-25-072-03 Siemens SIMATIC S7-1500 TM MFP ICSA-25-072-04 Siemens SiPass integrated AC5102/ACC-G2 and ACC-AP ICSA-25-072-05 Siemens SINAMICS S200 ICSA-25-072-06 Siemens SCALANCE LPE9403 ICSA-25-072-07 Siemens SCALANCE M-800 and SC-600 Families ICSA-25-072-08 Siemens Tecnomatix Plant Simulation ICSA-25-072-09 Siemens OPC UA ICSA-25-072-10 Siemens SINEMA Remote Connect Client ICSA-25-072-11 Siemens SIMATIC IPC Family, ITP1000, and Field PGs ICSA-25-072-12 Sungrow iSolarCloud Android App and WiNet Firmware ICSMA-25-072-01 Philips Intellispace Cardiovascular (ISCV) ICSA-25-070-01 Schneider Electric Uni-Telway Driver ICSA-25-070-02 Optigo Networks Visual BACnet Capture Tool/Optigo Visual Networks Capture Tool	https://www.cisa.gov/news-events/alerts/2025/03/11/cisa-releases-two-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2025/03/13/cisa-releases-thirteen-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2025/03/11/cisa-releases-two-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2025-24983 Microsoft Windows Win32k Use-After-Free Vulnerability CVE-2025-24984 Microsoft Windows NTFS Information Disclosure Vulnerability	https://www.cisa.gov/news-events/alerts/2025/03/11/cisa-adds-six-known-exploited-vulnerabilities-catalog

	CVE-2025-24985 Microsoft Windows Fast FAT File System Driver Integer Overflow Vulnerability CVE-2025-24991 Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability CVE-2025-24993 Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability CVE-2025-26633 Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability CVE-2025-24201 Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability CVE-2025-21590 Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability	https://www.cisa.gov/news-events/alerts/2025/03/13/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA and Partners Release Cybersecurity Advisory on Medusa Ransomware	#StopRansomware: Medusa Ransomware	https://www.cisa.gov/news-events/alerts/2025/03/12/cisa-and-partners-release-cybersecurity-advisory-medusa-ransomware

3 News

Σύντομη περιγραφή / Τίτλος	URL
Chinese Volt Typhoon Hackers Infiltrated US Electric Utility for Nearly a Year	https://hackread.com/chinese-volt-typhoon-hackers-infiltrated-us-electric-grid/
Microsoft: Recent Windows updates make USB printers print random text	https://www.bleepingcomputer.com/news/microsoft/microsoft-usb-printers-print-random-text-after-recent-windows-updates/

3.1 Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Cyberattack on Sunflower Medical Group and Multiple Healthcare Providers Suffer Data Breaches	https://dailysecurityreview.com/security-spotlight/cyberattack-on-sunflower-medical-group-and-multiple-healthcare-providers-suffer-data-breaches/
Telecom Giant NTT Admits Hackers Accessed 18,000 Corporate Customers Data	https://cybersecuritynews.com/telecom-giant-ntt-admits-hackers-accessed/

86,000+ Healthcare Staff Records Exposed from Misconfigured AWS S3 Bucket	https://cybersecuritynews.com/86000-healthcare-staff-records-exposed/

3.2 Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Severe authentication bypass vulnerability discovered in Perforce software	https://www.scworld.com/brief/severe-authentication-bypass-vulnerability-discovered-in-perforce-software
Over 400 IPs Exploiting Multiple SSRF Vulnerabilities in Coordinated Cyber Attack	https://thehackernews.com/2025/03/over-400-ips-exploiting-multiple-ssrf.html
New Ballista Botnet spreads using TP-Link flaw. Is it an Italian job?	https://securityaffairs.com/175278/malware/ballista-botnet-exploits-unpatched-tp-link-flaw.html
WordPress Vulnerability Expolited to Hack Moroccan Data Protection Authority Website	https://dailysecurityreview.com/security-spotlight/wordpress-vulnerability-expolited-to-hack-moroccan-data-protection-authority-website/
GraphQL Vulnerabilities: A Complete Guide to Security Testing and Advanced Exploitation Techniques	https://infosecwriteups.com/graphql-vulnerabilities-a-complete-guide-to-security-testing-and-advanced-exploitation-techniques-5eb94af945c0
Multiple Zoom Client Vulnerabilities Exposes Sensitive Data	https://cybersecuritynews.com/multiple-zoom-client-vulnerabilities/
Critical Windows Remote Desktop Services Vulnerability Lets Attackers Execute Malicious Code	https://cybersecuritynews.com/windows-remote-desktop-services-code-vulnerability/
Apache Camel Vulnerability Let Attackers Inject Arbitrary Headers – PoC Exploit Released	https://cybersecuritynews.com/apache-camel-vulnerability/
SolarWinds Web Help Desk Vulnerability Let Hackers Access Stored Passwords – PoC Released	https://cybersecuritynews.com/solar-winds-web-help-desk-vulnerability/
Apache Pinot Vulnerability Let Attackers Bypass Authentication	https://cybersecuritynews.com/apache-pinot-vulnerability/
Cisco Warns of IOS XR Software Vulnerability That Let Attackers Trigger DoS condition	https://cybersecuritynews.com/cisco-warns-of-ios-xr-software-vulnerability/
Apache NiFi Vulnerability Let Attackers Access MongoDB Username & Passwords	https://cybersecuritynews.com/apache-nifi-vulnerability-mongodb/
2-year-old Windows Kernel 0-day Vulnerability Exploited in the Wild	https://cybersecuritynews.com/microsoft-2-year-old-windows-kernel-0-day/
Tenda AC7 Routers Vulnerability Let Attackers Gain Root Shell With Malicious Payload	https://cybersecuritynews.com/tenda-ac7-routers-gain-root-shell/

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Patch Tuesday security updates for March 2025 fix six actively exploited zero-days	https://securityaffairs.com/175289/hacking/microsoft-patch-tuesday-security-updates-for-march-2025.html
iOS 18.3.2 Patches Actively Exploited WebKit Vulnerability	https://www.infosecurity-magazine.com/news/ios-1832-patches-exploited-webkit/
Microsoft patches Windows Kernel zero-day exploited since 2023	https://www.bleepingcomputer.com/news/microsoft/microsoft-patches-windows-kernel-zero-day-exploited-since-2023/
Mozilla warns users to update Firefox before certificate expires	https://www.bleepingcomputer.com/news/software/mozilla-warns-users-to-update-firefox-before-certificate-expires/
Actively exploited Apple zero-day addressed	https://www.scworld.com/brief/actively-exploited-apple-zero-day-addressed
March 2025 Patch Tuesday: Microsoft Fixes 57 Vulnerabilities, 7 Zero-Days	https://hackread.com/march-2025-patch-tuesday-microsoft-fixes-vulnerabilities-zero-days/
Windows 10 KB5053606 update fixes broken SSH connections	https://www.bleepingcomputer.com/news/microsoft/windows-10-kb5053606-update-fixes-broken-ssh-connections/
GitLab addressed critical auth bypass flaws in CE and EE	https://securityaffairs.com/175370/security/gitlab-addressed-critical-flaws-in-ce-and-ee.html
Fortinet Addresses Multiple Vulnerabilities in FortiSandbox, FortiOS, & Other Products	https://cybersecuritynews.com/fortinet-addresses-multiple-vulnerabilities/

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Medusa ransomware hit over 300 critical infrastructure organizations until February 2025	https://securityaffairs.com/175319/cyber-crime/medusa-ransomware-hit-over-300-critical-infrastructure-organizations-until-february-2025.html
China-linked APT UNC3886 targets EoL Juniper routers	https://securityaffairs.com/175308/apt/china-linked-apt-unc3886-targets-eol-juniper-routers.html
Android spyware 'KoSpy' spread by suspected North Korean APT	https://www.scworld.com/news/android-spyware-kospy-spread-by-suspected-north-korean-apt
Chinese Hackers Breach Juniper Networks Routers With Custom Backdoors and Rootkits	https://thehackernews.com/2025/03/chinese-hackers-breach-juniper-networks.html
One Million Devices Infected: Hackers Use Malvertising and GitHub to Spread Infostealers	https://www.infostealers.com/article/one-million-devices-infected-hackers-use-malvertising-and-github-to-spread-infostealers/
New SuperBlack ransomware exploits Fortinet auth bypass flaws	https://www.bleepingcomputer.com/news/security/new-superblack-ransomware-exploits-fortinet-auth-bypass-flaws/

CISA tags critical Ivanti EPM flaws as actively exploited in attacks	https://www.bleepingcomputer.com/news/security/cisa-tags-critical-ivanti-epm-flaws-as-actively-exploited-in-attacks/
New Botnet Dubbed “Eleven11bot” Hacked 30,000 Webcams	https://cybersecuritynews.com/new-botnet-dubbed-eleven11bot-hacked/
5000+ Malicious Packages Found In The Wild To Compromise Windows Systems	https://cybersecuritynews.com/5000-malicious-packages-found-in-the-wild/

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Modat launches premier product, Modat Magnify for Cybersecurity Professionals	https://hackread.com/modat-launches-premier-product-modat-magnify-for-cybersecurity-professionals/
Cybersecurity classics: 10 books that shaped the industry	https://www.helpnetsecurity.com/2025/03/13/cybersecurity-classics-books/
NetBird: Open-source network security	https://www.helpnetsecurity.com/2025/03/12/netbird-open-source-network-security/
New infosec products of the week: March 14, 2025	https://www.helpnetsecurity.com/2025/03/14/new-infosec-products-of-the-week-march-14-2025/
Decrypting Linux/ESXi Akira Ransomware Files Without Paying Ransomware	https://cybersecuritynews.com/decrypting-linux-esxi-akira-ransomware-files/

4 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.

5 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/