Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/03/2025 - 07/03/2025

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-2024-50707	10	Uniguest Tripleplay	Code Injection	before 24.2.1	N/A	https://uniguest.com/tripleplay/ https://uniguest.com/cve-bulletins/ https://uniguest.com/wp-content/uploads/2025/02/CVE-2024-50707-Vulnerability-Summary.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-25015	9.9	Kibana	Prototype Pollution	versions >= 8.15.0 and < 8.17.1 versions 8.17.1 and 8.17.2	N/A	https://www.elastic.co/kibana https://discuss.elastic.co/t/kibana-8-17-3-security-update-esa-2025-06/375441
https://nvd.nist.gov/vuln/detail/CVE-2025-1393	9.8	Weidmüller GTI Software	Use of Hard-coded Credentials	N/A	N/A	https://www.weidmueller-gti-software.com/en/services/cancellation_process/index.jsp https://certvde.com/en/advisories/VDE-2025-021
https://nvd.nist.gov/vuln/detail/CVE-2025-1316	9.8	Edimax IC-7100	OS Command Injection	N/A	N/A	https://www.edimax.com/edimax/download/download/data/edimax/au/download/for_home/home_legacy_products/home_legacy_ip_cameras_network_cameras/ic-7100 https://www.cisa.gov/news-events/ics-advisories/icsa-25-063-08
https://nvd.nist.gov/vuln/detail/CVE-2025-1932	9.8	Firefox and Thunderbird	Out-of-bounds Read	Firefox < 136, Firefox ESR < 128.8, Thunderbird < 136, and Thunderbird < 128.8	N/A	https://www.mozilla.org/el/firefox/new/ https://nvd.nist.gov/vuln/detail/CVE-2025-1932
https://nvd.nist.gov/vuln/detail/CVE-2025-25632	9.8	Tenda AC15	Command Injection	v15.03.05.19	N/A	https://www.smallnetbuilder.com/wireless/wireless-reviews/tenda-ac15-ac1900-smart-dual-band-gigabit-wifi-router-reviewed/ https://github.com/Pr0b1em/IoT/blob/master/TendaAC15v15.03.05.19telnet.md
https://nvd.nist.gov/vuln/detail/CVE-2025-22224	9.3	VMware ESXi	Time-of-check Time-of-use (TOCTOU) Race Condition	N/A	N/A	https://www.vmware.com/products/cloud-infrastructure/vsphere https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390
https://nvd.nist.gov/vuln/detail/CVE-2025-1260	9.1	Arista EOS	Improper Access Control	N/A	N/A	https://www.arista.com/en/products/eos https://www.arista.com/en/support/advisories-notices/security-advisory/21098-security-advisory-0111

https://nvd.nist.gov/vuln/detail/CVE-2025-27507	9	Zitadel	Authorization Bypass	N/A	N/A	https://zitadel.com/ https://github.com/zitadel/zitadel/security/advisories/GHSA-f3gh-529w-v32x
https://nvd.nist.gov/vuln/detail/CVE-2024-58045	8.6	HarmonyOS	Race Condition	N/A	N/A	https://www.harmonyos.com/en/ https://consumer.huawei.com/en/support/bulletin/2025/3/
https://nvd.nist.gov/vuln/detail/CVE-2024-48248	8.6	NAKIVO Backup & Replication	Absolute Path Traversal	before 11.0.0.88174	N/A	https://www.nakivo.com/ https://helpcenter.nakivo.com/Release-Notes/Content/Release-Notes.htm https://labs.watchtowr.com/the-best-security-is-when-we-all-agree-to-keep-everything-secret-except-the-secrets-nakivo-backup-replication-cve-2024-48248/
https://nvd.nist.gov/vuln/detail/CVE-2024-0114	8.1	NVIDIA Hopper HGX	Internal Asset Exposed to Unsafe Debug Access Level or State	N/A	N/A	https://www.nvidia.com/en-us/data-center/technologies/hopper-architecture/ https://nvidia.custhelp.com/app/answers/detail/a_id/5561
https://nvd.nist.gov/vuln/detail/CVE-2025-23368	8.1	Wildfly Elytron	Improper Restriction of Excessive Authentication Attempts	N/A	N/A	https://wildfly-security.github.io/wildfly-elytron/ https://access.redhat.com/security/cve/CVE-2025-23368
https://nvd.nist.gov/vuln/detail/CVE-2025-22447	7.8	RemoteView Agent (for Windows)	Incorrect Default Permissions	prior to v8.1.5.2	N/A	https://www.rview.com/en/ https://jvn.jp/en/jp/JVN24992507/
https://nvd.nist.gov/vuln/detail/CVE-2025-1702	7.5	Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress	SQL Injection	all versions up to, and including, 2.10.0	N/A	https://wordpress.org/plugins/ultimate-member/ https://www.wordfence.com/threat-intel/vulnerabilities/id/34adbae5-d615-4f8d-a845-6741d897f06c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-13320	7.5	CURCY - WooCommerce Multi Currency - Currency Switcher plugin for WordPress	SQL Injection	all versions up to, and including, 2.3.6	N/A	https://wordpress.org/plugins/woo-multi-currency/ https://www.wordfence.com/threat-intel/vulnerabilities/id/6d359a5c-db11-416e-a329-c3ed67b1a925?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-51476	7.5	IBM Concert Software	Improper Restriction of Excessive Authentication Attempts	1.0.5	N/A	https://www.ibm.com/products/concert https://www.ibm.com/support/pages/node/7184961

https://nvd.nist.gov/vuln/detail/CVE-2024-53458	7.5	Sysax Multi Server	Uncontrolled Resource Consumption	6.99	N/A	https://www.sysax.com/server/ https://packetstorm.news/files/id/182468 https://packetstormsecurity.com/files/182468/Sysax-Multi-Server-6.99-SSH-Denial-Of-Service.html
https://nvd.nist.gov/vuln/detail/CVE-2025-1702	7.5	Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress	SQL Injection	all versions up to, and including, 2.10.0	N/A	https://wordpress.org/plugins/ultimate-member/ https://www.wordfence.com/threat-intel/vulnerabilities/id/34adbae5-d615-4f8d-a845-6741d897f06c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-2003	7.1	Devolutions Server	Incorrect Authorization	2024.3.12 and earlier	N/A	https://devolutions.net/server/ https://devolutions.net/security/advisories/DEVO-2025-0003/
https://nvd.nist.gov/vuln/detail/CVE-2025-20206	7.1	Cisco Secure Client	Improper Verification of Cryptographic Signature	N/A	N/A	https://www.cisco.com/site/us/en/products/security/secure-client/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-dll-injection-AOyzEqSg

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Industrial Control Systems Advisories	ICSA-25-063-01 Carrier Block Load ICSA-25-063-02 Keysight Ixia Vision Product Family ICSA-25-063-03 Hitachi Energy MACH PS700 ICSA-25-063-04 Hitachi Energy XMC20 ICSA-25-063-05 Hitachi Energy UNEM/ECST ICSA-25-063-06 Delta Electronics CNCSoft-G2 ICSA-25-063-07 GMOD Apollo ICSA-25-063-08 Edimax IC-7100 IP Camera ICSA-25-065-01 Hitachi Energy PCU400 ICSA-25-065-02 Hitachi Energy Relion 670/650/SAM600-IO ICSA-25-037-02 Schneider Electric EcoStruxure (Update A)	https://www.cisa.gov/news-events/alerts/2025/03/04/cisa-releases-eight-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2025/03/06/cisa-releases-three-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2024-50302 Linux Kernel Use of Uninitialized Resource Vulnerability CVE-2025-22225 VMware ESXi Arbitrary Write Vulnerability CVE-2025-22224 VMware ESXi and Workstation TOCTOU Race Condition Vulnerability CVE-2025-22226 VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability	https://www.cisa.gov/news-events/alerts/2025/03/04/cisa-adds-four-known-exploited-vulnerabilities-catalog
FBI Warns of Data Extortion Scam Targeting Corporate Executives	Mail Scam Targeting Corporate Executives Claims Ties to Ransomware	https://www.cisa.gov/news-events/alerts/2025/03/06/fbi-warns-data-extortion-scam-targeting-corporate-executives

3 News

Σύντομη περιγραφή / Τίτλος	URL
New infosec products of the week: March 7, 2025	https://www.helpnetsecurity.com/2025/03/07/new-infosec-products-of-the-week-march-7-2025/
CISA Tags Windows and Cisco Vulnerabilities as Actively Exploited	https://dailysecurityreview.com/security-spotlight/cisa-tags-windows-and-cisco-vulnerabilities-as-actively-exploited/
PHP-CGI RCE Flaw Exploited in Attacks on Japan's Tech, Telecom, and E-Commerce Sectors	https://thehackernews.com/2025/03/php-cgi-rce-flaw-exploited-in-attacks.html
Google Announces GoStringUngarbler Tool to Decrypt Go Based Malware	https://cybersecuritynews.com/google-announces-gostringungarbler-tool/

3.1 Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Data breach at Japanese telecom giant NTT hits 18,000 companies	https://www.bleepingcomputer.com/news/security/data-breach-at-japanese-telecom-giant-ntt-hits-18-000-companies/

3.2 Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Vim Editor Vulnerability Exploited Via TAR Files to Trigger Code Execution	https://cybersecuritynews.com/vim-editor-vulnerability-exploited/
Cisco warns of Webex for BroadWorks flaw exposing credentials	https://www.bleepingcomputer.com/news/security/cisco-warns-of-webex-for-broadworks-flaw-exposing-credentials/
Critical Vulnerabilities in DrayTek Routers Exposes Devices to RCE Attack	https://cybersecuritynews.com/critical-vulnerabilities-in-draytek-routers-exposes-devices/
Multiple Jenkins Vulnerability Let Attackers Expose Secrets	https://cybersecuritynews.com/jenkins-vulnerability-expose-secrets/
Apache Pinot Vulnerability Let Remote Attackers Bypass Authentication	https://cybersecuritynews.com/apache-pinot-vulnerability-let-remote-attackers/
Cisco Secure Client for Windows Let Attackers Execute Arbitrary Code With SYSTEM Privileges	https://cybersecuritynews.com/cisco-secure-client-for-windows-vulnerability/
ZITADEL IDOR Vulnerabilities Let Attackers Modify Sensitive Settings	https://cybersecuritynews.com/zitadel-idor-vulnerabilities/
LibreOffice Vulnerability Let Attackers Execute Arbitrary Script Using Macro URL	https://cybersecuritynews.com/libreoffice-vulnerability-arbitrary-script/
Vulnerability in Chaty Pro Plugin Exposes 18,000 WordPress Sites	https://www.infosecurity-magazine.com/news/flaw-chaty-pro-plugin-18k/

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Chrome 134 Released, Fixes 14 Vulnerabilities That Could Crash the Browser	https://cybersecuritynews.com/chrome-134-released-fixes-14-vulnerabilities/
VMware Warns Customers to Patch Actively Exploited Zero-Day Vulnerabilities	https://www.infosecurity-magazine.com/news/vmware-patch-exploited-zero-day/
Elastic patches critical Kibana flaw allowing code execution	https://securityaffairs.com/174999/security/elastic-kibana-critical-flaw.html

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Warns of Malvertising Campaign Infecting Over 1 Million Devices Worldwide	https://thehackernews.com/2025/03/microsoft-warns-of-malvertising.html
Ransomware gang encrypted network from a webcam to bypass EDR	https://www.bleepingcomputer.com/news/security/ransomware-gang-encrypted-network-from-a-webcam-to-bypass-edr/
New polyglot malware hits aviation, satellite communication firms	https://www.bleepingcomputer.com/news/security/new-polyglot-malware-hits-aviation-satellite-communication-firms/
Beware of Fake Tax Claims that Tricks Users to Steal Over $10,000 From Victims	https://cybersecuritynews.com/beware-of-fake-tax-claims-that-tricks-users/
China-Linked Silk Typhoon Expands Cyber Attacks to IT Supply Chains for Initial Access	https://thehackernews.com/2025/03/china-linked-silk-typhoon-expands-cyber.html
Misconfigured Apache Airflow Servers Exposes Login Credentials to Hackers	https://cybersecuritynews.com/misconfigured-apache-airflow-servers/
APT group uses OneDrive in cyber espionage vs Russia	https://www.scworld.com/brief/apt-group-uses-onedrive-in-cyber-espionage-vs-russia
Six Critical Infrastructure Sectors Failing on NIS2 Compliance	https://www.infosecurity-magazine.com/news/critical-infrastructure-sectors/
Over 37,000 VMware ESXi servers vulnerable to ongoing attacks	https://www.bleepingcomputer.com/news/security/over-37-000-vmware-esxi-servers-vulnerable-to-ongoing-attacks/
Silk Typhoon Hackers Now Target IT Supply Chains to Breach Networks	https://dailysecurityreview.com/security-spotlight/silk-typhoon-hackers-now-target-it-supply-chains-to-breach-networks/
BadBox Malware Disrupted on 500K Infected Android Devices	https://dailysecurityreview.com/security-spotlight/badbox-malware-disrupted-on-500k-infected-android-devices/
Android App With 220,000+ Downloads From Google Play Installs Banking Trojan	https://cybersecuritynews.com/android-app-with-220000-downloads/
BadBox Malware from Google Play Hacked 50,000+ Android Devices Using 24 Apps	https://cybersecuritynews.com/badbox-from-google-play-hacked-50000-android-devices/
49,000+ Access Management Systems Worldwide Configured With Massive Security Gaps	https://cybersecuritynews.com/49000-access-management-systems-exposed/

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
The 5 stages of incident response grief	https://www.helpnetsecurity.com/2025/03/05/incident-response-grief-stages/
Best Browser Extensions for Bug Hunting and Cybersecurity	https://infosecwriteups.com/best-browser-extensions-for-bug-hunting-and-cybersecurity-77faf6bd8188
The CISO’s bookshelf: 10 must-reads for security leaders	https://www.helpnetsecurity.com/2025/03/06/ciso-books-must-reads-for-security-leaders/
Open-Source Tool Rayhunter Helps Users Detect Stingray Attacks	https://dailysecurityreview.com/security-spotlight/open-source-tool-rayhunter-helps-users-detect-stingray-attacks/
15 Best Patch Management Tools In 2025	https://cybersecuritynews.com/patch-management-tools/

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/