Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 28/012024 - 31/01/2025

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-2025-20061	9.8	mySCADA myPRO	OS Command Injection	N/A	N/A	https://www.myscada.org/mypro/ https://www.cisa.gov/news-events/ics-advisories/icsa-25-023-01
https://nvd.nist.gov/vuln/detail/CVE-2025-21311	9.8	Windows NTLM V1	Elevation of Privilege	N/A	N/A	https://support.microsoft.com/en-us/topic/security-guidance-for-ntlmv1-and-lm-network-authentication-da2168b6-4a31-0088-fb03-f081acde6e73 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21311
https://nvd.nist.gov/vuln/detail/CVE-2025-21298	9.8	Windows OLE	Remote Code Execution	N/A	N/A	https://learn.microsoft.com/en-us/cpp/mfc/ole-background?view=msvc-170 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21298
https://nvd.nist.gov/vuln/detail/CVE-2023-29268	9.8	Splus Server component of TIBCO Software	Unrestricted File Upload	11.4.10 and below, versions 11.5.0, 11.6.0, 11.6.1, 11.6.2, 11.7.0, 11.8.0, 11.8.1, 12.0.0, 12.0.1, and 12.0.2, versions 12.1.0 and 12.2.0	N/A	https://www.tibco.com/ https://www.tibco.com/services/support/advisories
https://nvd.nist.gov/vuln/detail/CVE-2023-30546	9.8	Contiki-NG (operating system for Internet of Things)	off-by-one error	4.8 and prior	N/A	https://www.contiki-ng.org/ https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-257g-w39m-5jj4
https://nvd.nist.gov/vuln/detail/CVE-2024-48852	9.4	FLEXON	Insertion of Sensitive Information into Log File	through <= 9.3.4	N/A	https://new.abb.com/low-voltage/products/building-automation/product-range/abb-cylon/products-and-downloads/highlights/flxeon-series https://search.abb.com/library/Download.aspx?DocumentID=9AKK108470A5684&LanguageCode=en&DocumentPartId=PDF&Action=Launch
https://nvd.nist.gov/vuln/detail/CVE-2025-0762	8.8	Google Chrome	Use After Free	prior to 132.0.6834.159	N/A	https://www.google.com/chrome https://chromereleases.googleblog.com/2025/01/stable-

						channel-update-for-desktop_28.html https://issues.chromium.org/issues/384844003
https://nvd.nist.gov/vuln/detail/CVE-2024-55968	8.8	DTEX Forwarder	Use of Hard-coded Credentials	6.1.1	N/A	https://www.dtexsystems.com/ https://www.tenable.com/cve/CVE-2024-55968
https://nvd.nist.gov/vuln/detail/CVE-2024-57376	8.8	D-Link DSR-150 DSR-150, DSR-150N, DSR-250, DSR-250N, DSR-500N, DSR-1000N	Classic Buffer Overflow	from 3.13 to 3.17B901C	N/A	https://www.dlink.com https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2024-52875	8.8	GFI Kerio Control	Reflected Cross-Site Scripting (XSS)	9.2.5 through 9.4.5	N/A	https://gfi.ai/products-and-solutions/network-security-solutions/keriocontrol https://karmainsecurity.com/hacking-kerio-control-via-cve-2024-52875
https://nvd.nist.gov/vuln/detail/CVE-2024-1991	8.8	RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login plugin for WordPress	privilege escalation	all versions up to, and including, 5.3.0.0	N/A	https://el.wordpress.org/plugins/custom-registration-form-builder-with-submission-manager/ https://www.wordfence.com/threat-intel/vulnerabilities/id/766e3966-157a-4db3-9179-813032343f76?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2023-22919	8.8	Zyxel NBG6604	post-authentication command injection	firmware version V1.01(ABIR.0)C0	N/A	https://download.zyxel.com/NBG6604/user_guide/NBG6604_v1_ed3.pdf https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerability-in-nbg6604-home-router
https://nvd.nist.gov/vuln/detail/CVE-2025-22217	8.6	Vmware Avi Load Balancer	SQL Injection	N/A	N/A	https://www.vmware.com/products/cloud-infrastructure/avi-load-balancer https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25346
https://nvd.nist.gov/vuln/detail/CVE-2022-41736	8.4	IBM Spectrum Scale Container Native Storage Access	unspecified vulnerability that could allow a local user to obtain root privileges	5.1.2.1 through 5.1.6.0	N/A	https://www.ibm.com/docs/en/STXKQY_CNS_SHR_5.2.1/pdf/scale_cns_521x.pdf https://www.ibm.com/support/pages/node/6964564
https://nvd.nist.gov/vuln/detail/CVE-2024-13484	8.2	ArgoCD	Exposure of Resource to Wrong Sphere	N/A	N/A	https://argo-cd.readthedocs.io/en/stable/ https://access.redhat.com/security/cve/CVE-2024-13484
https://nvd.nist.gov/vuln/detail/CVE-2024-41140	8.1	Zohocorp ManageEngine Applications Manager	Incorrect Authorization	174000 and prior	N/A	https://www.manageengine.com/products/applications_manager/ https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2024-41140.html

https://nvd.nist.gov/vuln/detail/CVE-2025-0798	8.1	MicroWorld eScan Antivirus	Command Injection	7.0.32 on Linux	N/A	https://escanav.com/en/ https://github.com/dmknght/FIS_RnD/blob/main/escan_rtscanner_rce.md
https://nvd.nist.gov/vuln/detail/CVE-2025-23374	8	Dell Networking Switches	Insertion of Sensitive Information into Log File	SONiC OS, version(s) prior to 4.4.1 and 4.2.3	N/A	https://www.dell.com/en-us/dt/networking/index.htm#tab0=0 https://www.dell.com/support/kbdoc/en-us/000278568/dsa-2025-057-security-update-for-dell-enterprise-sonic-distribution-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2025-24527	8	Akamai Enterprise Application Access	Incorrect Permission Assignment for Critical Resource	before 2025-01-17	N/A	https://www.akamai.com/products/enterprise-application-access https://techdocs.akamai.com/eaa/changelog/january-29-2024
https://nvd.nist.gov/vuln/detail/CVE-2025-0834	7.8	Wondershare Dr.Fone	Improper Privilege Management	13.5.21	N/A	https://drfone.wondershare.net https://www.incibe.es/en/incibe-cert/notices/aviso/wondershare-drfone-privilege-scalation-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2025-23385	7.8	JetBrains ReSharper	Process Control	ReSharper before 2024.3.4, 2024.2.8, and 2024.1.7, Rider before 2024.3.4, 2024.2.8, and 2024.1.7, dotTrace before 2024.3.4, 2024.2.8, and 2024.1.7, ETW Host Service before 16.43	N/A	https://www.jetbrains.com/resharper/ https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2025-21107	7.8	Dell NetWorker,	Unquoted Search Path or Element	prior to 19.11.0.3, all versions of 19.10 & prior versions	N/A	https://www.dell.com/en-us/lp/dt/data-protection-suite-networker-data-protection-software https://www.dell.com/support/kbdoc/en-us/000278811/dsa-2025-064-security-update-for-dell-networker-networker-virtual-edition-and-networker-management-console-multiple-component-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-12705	7.5	BIND 9	Allocation of Resources Without Limits or Throttling	9.18.0 through 9.18.32, 9.20.0 through 9.20.4, 9.21.0 through 9.21.3, and 9.18.11-S1 through 9.18.32-S1	N/A	https://bind9.net/ https://kb.isc.org/docs/cve-2024-12705
https://nvd.nist.gov/vuln/detail/CVE-2024-7695	7.5	MOXA products (Multiple switches)	Out-of-bounds Write	N/A	N/A	https://www.moxa.com/en https://www.moxa.com/en/support/product-support/security-advisory/mpsa-240162-cve-2024-7695-out-of-bounds-write-vulnerability-identified-in-multiple-pt-switches

https://nvd.nist.gov/vuln/detail/CVE-2024-57519	7.5	Open5GS	Allocation of Resources Without Limits or Throttling	v.2.7.2	N/A	https://open5gs.org/ https://github.com/f4rs1ght/vuln-research/tree/main/CVE-2024-57519
https://nvd.nist.gov/vuln/detail/CVE-2024-56529	7.5	Mailcow	Session Fixation	through 2024-11b	N/A	https://mailcow.email/ https://github.com/mailcow/mailcow-dockerized/security/advisories/GHSA-23c8-4wwr-g3c6
https://nvd.nist.gov/vuln/detail/CVE-2023-2360	7.5	Acronis Cyber Infrastructure (ACI)	Sensitive information disclosure	before build 5.2.0-135	N/A	https://www.acronis.com/en-eu/products/cyber-infrastructure/ https://security-advisory.acronis.com/advisories/SEC-4215
https://nvd.nist.gov/vuln/detail/CVE-2024-22429	7.5	Dell BIOS	Improper Input Validation	N/A	N/A	https://www.dell.com/support/contents/el-gr/article/product-support/self-support-knowledgebase/fix-common-issues/bios-uefi https://www.dell.com/support/kbdoc/en-us/000221102/dsa-2024-020
https://nvd.nist.gov/vuln/detail/CVE-2025-21399	7.4	Microsoft Edge (Chromium-based)	Elevation of Privilege	N/A	N/A	https://www.microsoft.com/en-us/edge https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21399
https://www.cve.org/CVERecord?id=CVE-2024-13472	7.3	The WooCommerce Product Table Lite plugin for WordPress	Unauthenticated Arbitrary Shortcode Execution & Reflected Cross-Site Scripting	all versions up to, and including, 3.9.4	N/A	https://wordpress.org/plugins/wc-product-table-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4f1a1171-3d7b-46a4-982e-fe318e3017b7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-24458	7.1	JetBrains YouTrack	account takeover was possible via spoofed email and Helpdesk integration	before 2024.3.55417	N/A	https://www.jetbrains.com/youtrack https://www.jetbrains.com/privacy-security/issues-fixed/

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Known Exploited Vulnerability to Catalog	CVE-2025-24085 Apple Multiple Products Use-After-Free Vulnerability	https://www.cisa.gov/news-events/alerts/2025/01/29/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Industrial Control Systems Advisories	ICSA-25-028-01 B&R Automation Runtime ICSA-25-028-02 Schneider Electric Power Logic ICSA-25-028-03 Rockwell Automation FactoryTalk ICSA-25-028-04 Rockwell Automation FactoryTalk View Site Edition ICSA-25-028-05 Rockwell Automation DataMosaix Private Cloud ICSA-25-028-06 Schneider Electric RemoteConnect and SCADAPack x70 Utilities ICSMA-24-352-01 BD Diagnostic Solutions Products (Update A) ICSA-25-030-01 Hitachi Energy UNEM ICSA-25-030-02 New Rock Technologies Cloud Connected Devices ICSA-25-030-03 Schneider Electric System Monitor Application in Harmony and Pro-face PS5000 Legacy Industrial PCs ICSA-25-030-04 Rockwell Automation KEPServer ICSA-25-030-05 Rockwell Automation FactoryTalk AssetCentre ICSMA-25-030-01 Contec Health CMS8000 Patient Monitor ICSA-24-135-04 Mitsubishi Electric Multiple FA Engineering Software Products (Update B) ICSMA-22-244-01 Contec Health CMS8000 Patient Monitor (Update A)	https://www.cisa.gov/news-events/alerts/2025/01/28/cisa-releases-seven-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2025/01/30/cisa-releases-eight-industrial-control-systems-advisories
Vulnerability Summary for the Week of January 20, 2025	Common Vulnerabilities and Exposures (CVE)	https://www.cisa.gov/news-events/bulletins/sb25-026

3 News

Σύντομη περιγραφή / Τίτλος	URL
Scores of Critical UK Government IT Systems Have Major Security Holes	https://www.infosecurity-magazine.com/news/scores-critical-government-it/
Ransomware Attack Disrupts Blood Donation Services in US	https://www.infosecurity-magazine.com/news/ransomware-blood-donation-services/
Google blocked 2.36 million risky Android apps from Play Store in 2024	https://www.bleepingcomputer.com/news/security/google-blocked-236-million-risky-android-apps-from-play-store-in-2024/

3.1 Breaches

Σύντομη περιγραφή / Τίτλος	URL
OAuth Flaw Exposed Millions of Airline Users to Account Takeovers	https://www.darkreading.com/application-security/oauth-flaw-exposed-millions-airline-users-account-takeovers
Hackers Claim 2nd Breach at HP Enterprise, Plan to Sell Access	https://hackread.com/hackers-claim-2nd-breach-hp-enterprise-sell-access/
DeepSeek Exposed Database Leaks Sensitive Data	https://www.infosecurity-magazine.com/news/deepseek-database-leaks-sensitive/
US healthcare provider data breach impacts 1 million patients	https://www.bleepingcomputer.com/news/security/us-healthcare-provider-data-breach-impacts-1-million-patients/

3.2 Vulnerabilities and flaws

Σύντομη περιγραφή / Τίτλος	URL
AMD acknowledges microcode vulnerability	https://www.scworld.com/brief/amd-acknowledges-microcode-vulnerability
Critical remote code execution bug found in Cacti framework	https://securityaffairs.com/173597/security/critical-rce-cacti-framework.html
Clone2Leak Attacks Exploit Git Flaws to Steal Credentials	https://dailysecurityreview.com/security-spotlight/clone2leak-attacks-exploit-git-flaws-to-steal-credentials/
PHP package Voyager flaws expose to one-click RCE exploits	https://securityaffairs.com/173646/hacking/php-package-voyager-flaws.html
New Aquabot Botnet Exploits CVE-2024-41710 in Mitel Phones for DDoS Attacks	https://thehackernews.com/2025/01/new-aquabot-botnet-exploits-cve-2024.html
Unpatched Zyxel CPE Zero-Day Pummeled by Cyberattackers	https://www.darkreading.com/endpoint-security/unpatched-zyxel-cpe-zero-day-cyberattackers
Whatsup Gold, Observium and Offis vulnerabilities	https://blog.talosintelligence.com/whatsup-gold-observium-offis-vulnerabilities/
Zyxel zero-day flaw actively being exploited	https://www.scworld.com/brief/zyxel-zero-day-flaw-actively-being-exploited
Cisco’s Webex Chat Vulnerabilities Let Attackers Access Organizations Chat Histories	https://cybersecuritynews.com/ciscos-webex-chat-vulnerabilities/

D-Link Routers Vulnerability Let Attackers Gain Full Router Control Remotely	https://cybersecuritynews.com/d-link-routers-attackers-router-remotely/
VMware Aria Operations Vulnerabilities Let Attackers Perform Admin Operations	https://cybersecuritynews.com/vmware-aria-operations-vulnerabilities-admin/

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
VMware fixed a flaw in Avi Load Balancer	https://securityaffairs.com/173569/security/vmware-fixed-avi-load-balancer-flaw.html
Microsoft urges updates to outdated Exchange servers	https://www.scworld.com/brief/microsoft-urges-updates-to-outdated-exchange-servers
Patch coming for reported firmware bugs in Palo Alto firewalls	https://www.scworld.com/brief/patch-coming-for-reported-firmware-bugs-in-palo-alto-firewalls
TeamViewer fixed a vulnerability in Windows client and host applications	https://securityaffairs.com/173658/security/teamviewer-windows-client-flaw.html
Broadcom fixed information disclosure flaws in VMware Aria Operations	https://securityaffairs.com/173677/security/vmware-aria-operations-flaws.html

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Europeans targeted with new Tor-using backdoor and infostealers	https://www.helpnetsecurity.com/2025/01/28/tornet-tor-backdoor-infostealers/
Russian UAC-0063 Targets Europe and Central Asia with Advanced Malware	https://hackread.com/russian-uac-0063-europe-central-asia-advanced-malware/
Tata Technologies Hit by Ransomware Attack	https://www.infosecurity-magazine.com/news/tata-technologies-ransomware-attack/
CISA and FDA Warn of Critical Backdoor in Contec CMS8000 Patient Monitors	https://thehackernews.com/2025/01/cisa-and-fda-warn-of-critical-backdoor.html
Fake DeepSeek Campaign Attacking macOS Users to Deliver Poseidon Malware	https://cybersecuritynews.com/deepseek-campaign-attacking-macos-users/
Coyote Banking Malware Weaponizing Windows LNK Files To Execute Malicious Scripts	https://cybersecuritynews.com/coyote-banking-malware-weaponizing-windows-lnk-files/
TAG-124 Hacked 1000+ WordPress Sites To Embed Payloads	https://cybersecuritynews.com/tag-124-hacked-1000-wordpress-sites/
Hackers Abusing GitHub Infrastructure to Deliver Lumma Stealer	https://debricked.com/vulnerability-database?page=2
New Android Malware Exploiting Wedding Invitations to Steal Victims WhatsApp Messages	https://cybersecuritynews.com/new-android-malware-exploiting-wedding-invitations/
Hackers Exploit Public-facing Vulnerable IIS, Apache, SQL Servers to Attack Gov & Telcom Networks	https://cybersecuritynews.com/hackers-exploit-public-facing-vulnerable-iis-apache-sql-servers/

Hackers Use 10,000 WordPress Sites To Deliver Malware To macOS and Microsoft Systems	https://cybersecuritynews.com/hackers-use-10000-wordpress-sites-to-deliver-malware/

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Opengrep : A Hype and Marketing Gimmick, let's rename it to Privategrep.	https://rohitcoder.medium.com/opengrep-a-hype-and-marketing-gimmick-lets-rename-it-to-privategrep-61225dbf9090
Infosec products of the month: January 2025	https://www.helpnetsecurity.com/2025/01/31/infosec-products-of-the-month-january-2025/
OPNsense 25.1 Released With Improved Security Zones & FreeBSD 14.2 Plus	https://cybersecuritynews.com/opnsense-25-1-released/

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/