Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 21/012024 - 24/01/2025

Contents

1 Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	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-2025-20156	9.9	Cisco Meeting Management	Improper Handling of Insufficient Privileges	N/A	N/A	https://www.cisco.com/c/en/us/support/conferencing/meeting-management/series.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-ole2-H549rphA https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-privesc-uy2Vf8pc
https://nvd.nist.gov/vuln/detail/CVE-2025-21556	9.9	Oracle Agile PLM Framework product of Oracle Supply Chain	allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM	9.3.6	N/A	https://www.oracle.com/scm/product-lifecycle-management/ https://www.oracle.com/security-alerts/cpujan2025.html
https://nvd.nist.gov/vuln/detail/CVE-2024-12857	9.8	AdForest theme for WordPress	Authentication Bypass	all versions up to, and including, 5.1.8	N/A	https://themeforest.net/item/adforest-classified-wordpress-theme/19481695 https://www.wordfence.com/threat-intel/vulnerabilities/id/4ff3b4f1-dd36-43d0-b472-55a940907437?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-13091	9.8	WPBot Pro Wordpress Chatbot plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 13.5.4	N/A	https://wordpress.org/plugins/chatbot/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0f9b6979-2662-4d2f-9656-b880dd80832c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-49748	9.8	Android (multiple vulnerabilities)	Out-of-bounds Write	N/A	N/A	https://source.android.com/ https://source.android.com/docs/security/bulletin/2025-01-01
https://nvd.nist.gov/vuln/detail/CVE-2025-21535	9.8	Oracle WebLogic Server product of Oracle Fusion Middleware	Missing Authentication for Critical Function	12.2.1.4.0 and 14.1.1.0.0	N/A	https://www.oracle.com/java/weblogic/ https://www.oracle.com/security-alerts/cpujan2025.html
https://nvd.nist.gov/vuln/detail/CVE-2025-21524	9.8	Oracle JD Edwards	allows unauthenticated attacker with network access via	Prior to 9.2.9.0	N/A	https://www.oracle.com/applications/jd-edwards-enterpriseone/ https://www.oracle.com/security-alerts/cpujan2025.html

CVE	Score	Product	Vulnerability Type	Affected Versions		References
			HTTP to compromise the product			
https://nvd.nist.gov/vuln/detail/CVE-2025-23006	9.8	SMA1000 Appliance Management Console (AMC)	Deserialization of Untrusted Data	N/A	N/A	https://www.sonicwall.com/support/technical-documentation/docs/sma_1000-12-4-deployment_planning_guide/Content/About_SonicWall_Secure_Mobile_Access/appliance-management-console.htm https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002
https://nvd.nist.gov/vuln/detail/CVE-2025-21547	9.1	Oracle Hospitality OPERA 5	Allocation of Resources Without Limits or Throttling	5.6.19.20, 5.6.25.8, 5.6.26.6 and 5.6.27.1	N/A	https://www.oracle.com/hospitality/products/opera-property-services/ https://www.oracle.com/security-alerts/cpujan2025.html
https://nvd.nist.gov/vuln/detail/CVE-2024-54794	9.1	SpagoBI	Command Injection	3.5.1	N/A	https://spagobi.readthedocs.io/en/latest/ https://github.com/MarioTesoro/CVE-2024-54794
https://nvd.nist.gov/vuln/detail/CVE-2024-55573	9.1	Centreon centreon-web	SQL injection	24.10.x before 24.10.3, 24.04.x before 24.04.9, 23.10.x before 23.10.19, 23.04.x before 23.04.24	N/A	https://www.centreon.com/ https://github.com/centreon/centreon/releases https://thewatch.centreon.com/latest-security-bulletins-64/cve-2024-55573-centreon-web-critical-severity-4264
https://nvd.nist.gov/vuln/detail/CVE-2025-23921	9	Gravity Forms	Unrestricted Upload of File with Dangerous Type	from n/a through 1.1.3	N/A	https://www.gravityforms.com/ https://patchstack.com/database/wordpress/plugin/gf-multi-uploader/vulnerability/wordpress-multi-uploader-for-gravity-forms-plugin-1-1-3-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-52975	9	Fleet Server	Exposure of Sensitive Information to an Unauthorized Actor	N/A	N/A	https://www.elastic.co/guide/en/fleet/current/fleet-server.html https://discuss.elastic.co/t/fleet-server-8-15-0-security-update-esa-2024-31/373522
https://nvd.nist.gov/vuln/detail/CVE-2024-31903	8.8	IBM Sterling B2B Integrator Standard Edition	Deserialization of Untrusted Data	6.0.0.0 through 6.1.2.5 and 6.2.0.0 through 6.2.0.2	N/A	https://www.ibm.com/products/b2b-integration-saas/standard https://www.ibm.com/support/pages/node/7172233
https://nvd.nist.gov/vuln/detail/CVE-2024-57542	8.8	Linksys E8450	OS Command Injection	v1.2.00.360516	N/A	https://support.linksys.com/kb/article/504-en/ https://github.com/Wood1314/Linksys_E8450_vul/blob/main/4/4.md
https://nvd.nist.gov/vuln/detail/CVE-2024-10936	8.8	String locator plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 2.6.6	N/A	https://wordpress.org/plugins/string-locator/ https://www.wordfence.com/threat-intel/vulnerabilities/id/1404f034-2d1d-44b2-87e5-61f72f215417?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-23011	8.8	Fedora Repository	Relative Path Traversal	3.8.1	N/A	https://fedorarepository.org/ https://github.com/fcrepo-exts/migration-utils https://github.com/fcrepo/fcrepo/releases

CVE	Score	Product	Vulnerability	Affected Version	Fixed Version	References
						https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2025/va-25-021-01.json
https://nvd.nist.gov/vuln/detail/CVE-2025-24399 https://nvd.nist.gov/vuln/detail/CVE-2025-24398	8.8	Jenkins OpenId Connect Authentication Plugin Jenkins Bitbucket Server Integration Plugin	Incorrect Default Permissions Cross-Site Request Forgery (CSRF)	4.452.v2849b_d3945fa_ and earlier, 2.1.0 through 4.1.3 (both inclusive)	except 4.438.440.v3f5f201de5dc N/A	https://plugins.jenkins.io/oic-auth/ https://plugins.jenkins.io/atlassian-bitbucket-server-integration/ https://www.jenkins.io/security/advisory/2025-01-22/#SECURITY-3461 https://www.jenkins.io/security/advisory/2025-01-22/#SECURITY-3434
https://nvd.nist.gov/vuln/detail/CVE-2023-50733	8.6	Lexmark devices	Improper Input Validation	N/A	N/A	https://www.lexmark.com/en_US/products/series/printer-and-multifunction/finder.shtml https://www.lexmark.com/en_us/solutions/security/lexmark-security-advisories.html
https://nvd.nist.gov/vuln/detail/CVE-2025-23477	8.2	Realty Workstation	Missing Authorization	from n/a through 1.0.45	N/A	https://www.realtyworkstation.com/ https://patchstack.com/database/wordpress/plugin/realty-workstation/vulnerability/wordpress-realty-workstation-plugin-1-0-45-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-21516	8.1	Oracle E-Business Suite	Incorrect Authorization	12.2.5-12.2.13	N/A	https://www.oracle.com/applications/ebusiness/ https://www.oracle.com/security-alerts/cpujan2025.html
https://nvd.nist.gov/vuln/detail/CVE-2025-0650	8.1	Open Virtual Network (OVN)	Improper Access Control	N/A	N/A	https://www.ovn.org/en/ https://access.redhat.com/security/cve/CVE-2025-0650
https://nvd.nist.gov/vuln/detail/CVE-2025-21532	7.8	Oracle Analytics Desktop	Incorrect Authorization	Prior to 8.1.0	N/A	https://www.oracle.com/solutions/business-analytics/analytics-desktop/oracle-analytics-desktop.html https://www.oracle.com/security-alerts/cpujan2025.html
https://nvd.nist.gov/vuln/detail/CVE-2025-20165	7.5	Cisco BroadWorks	Memory Allocation with Excessive Size Value	N/A	N/A	https://www.cisco.com/c/en/us/products/unified-communications/broadworks/index.html https://blog.clamav.net/2025/01/clamav-142-and-108-security-patch.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-sip-dos-mSySbrmt https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-ole2-H549rphA
https://nvd.nist.gov/vuln/detail/CVE-2025-22450	7.5	iodata devices (UD-LT2)	Inclusion of Undocumented Features or Chicken Bits	firmware Ver.1.00.008_SE and earlier	N/A	https://www.iodata.com/ https://jvn.jp/en/jp/JVN15293958/
https://nvd.nist.gov/vuln/detail/CVE-2025-21545	7.5	Oracle PeopleSoft	Allocation of Resources Without Limits or Throttling	8.60 and 8.61	N/A	https://www.oracle.com/applications/peoplesoft/ https://www.oracle.com/security-alerts/cpujan2025.html

Reference	CVSS	Product	Vulnerability	Affected Version	Fixed Version	Additional References
https://nvd.nist.gov/vuln/detail/CVE-2025-21521	7.5	Oracle MySQL	Allocation of Resources Without Limits or Throttling	8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior	N/A	https://www.mysql.com/ https://www.oracle.com/security-alerts/cpujan2025.html
https://nvd.nist.gov/vuln/detail/CVE-2025-21571	7.3	Oracle VM VirtualBox	unauthorized creation, deletion or modification access to critical data	Prior to 7.0.24 and prior to 7.1.6	N/A	https://www.virtualbox.org/ https://www.oracle.com/security-alerts/cpujan2025.html
https://nvd.nist.gov/vuln/detail/CVE-2024-56924	7.3	Code Astro Internet banking system	Cross-Site Request Forgery (CSRF)	2.0.0	N/A	https://codeastro.com/internet-banking-system-in-php-with-source-code/ (not available right now 24-01-2025) https://github.com/ipratheep/CVE-2024-56924 https://github.com/ipratheep/CVE-2024-56924
https://nvd.nist.gov/vuln/detail/CVE-2025-24458	7.1	JetBrains YouTrack	Authentication Bypass by Spoofing	before 2024.3.55417	N/A	https://www.jetbrains.com/youtrack/ https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2025-24030	7.1	Envoy Gateway	Unprotected Primary Channel	prior to 1.2.6	1.2.6	https://gateway.envoyproxy.io/ https://www.envoyproxy.io/docs/envoy/latest/configuration/best_practices/edge https://www.envoyproxy.io/docs/envoy/latest/operations/admin

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications	CVE-2025-0282 and CVE-2025-0283	https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-022a
CISA Releases Industrial Control Systems Advisories	ICSA-25-021-01 Traffic Alert and Collision Avoidance System (TCAS) II ICSA-25-021-02 Siemens SIMATIC S7-1200 CPUs ICSA-25-021-03 ZF Roll Stability Support Plus (RSSPlus) ICSA-25-023-01 mySCADA myPRO Manager ICSA-25-023-02 Hitachi Energy RTU500 Series Product ICSA-25-023-03 Schneider Electric EVlink Home Smart and Schneider Charge ICSA-25-023-04 Schneider Electric Easergy Studio ICSA-25-023-05 Schneider Electric EcoStruxure Power Build Rapsody ICSA-25-023-06 HMS Networks Ewon Flexy 202	https://www.cisa.gov/news-events/alerts/2025/01/21/cisa-releases-three-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2025/01/23/cisa-releases-six-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerability to Catalog	CVE-2020-11023 JQuery Cross-Site Scripting (XSS) Vulnerability	https://www.cisa.gov/news-events/alerts/2025/01/23/cisa-adds-one-known-exploited-vulnerability-catalog
Vulnerability Summary for the Week of January 13, 2025	Common Vulnerabilities and Exposures	https://www.cisa.gov/news-events/bulletins/sb25-021

3 News

Σύντομη περιγραφή / Τίτλος	URL
Hackers exploit 16 zero-days on first day of Pwn2Own Automotive 2025	https://www.bleepingcomputer.com/news/security/hackers-exploit-16-zero-days-on-first-day-of-pwn2own-automotive-2025/
73% of UK Education Sector Hit by Cyber-Attacks in Past Five Years	https://www.infosecurity-magazine.com/news/schools-hit-by-cyberattacks-in/
48,000+ internet-facing Fortinet firewalls still open to attack	https://www.helpnetsecurity.com/2025/01/22/48000-internet-facing-fortinet-firewalls-still-open-to-attack/
Cloudflare Mitigates Record-Breaking 5.6Tbps DDoS Attack	https://www.infosecurity-magazine.com/news/cloudflare-mitigates-record/
GDPR Fines Total €1.2bn in 2024	https://www.infosecurity-magazine.com/news/gdpr-fines-total-2024/
13,000 MikroTik Routers Hijacked by Botnet for Malspam and Cyberattacks	https://thehackernews.com/2025/01/13000-mikrotik-routers-hijacked-by.html
Microsoft: Exchange 2016 and 2019 reach end of support in October	https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-2016-and-2019-reach-end-of-support-in-october/
GhostGPT offers AI coding, phishing assistance for cybercriminals	https://www.scworld.com/news/ghostgpt-offers-ai-coding-phishing-assistance-for-cybercriminals

| 84% of Healthcare Organizations Spotted a Cyberattack in the Late Year | https://www.darkreading.com/threat-intelligence/84-of-healthcare-organizations-spotted-a-cyberattack-in-the-late-year |

3.1 Breaches

Σύντομη περιγραφή / Τίτλος	URL
IPany VPN breached in supply-chain attack to push custom malware	https://www.bleepingcomputer.com/news/security/ipany-vpn-breached-in-supply-chain-attack-to-push-custom-malware/
HPE Data Breached by IntelBroker: HPE Data on Sale on Dark Web	https://dailysecurityreview.com/security-spotlight/hpe-data-breached-by-intelbroker-hpe-data-on-sale-on-dark-web/
ICICI Bank Data Breach – BASHE Ransomware Group Allegedly Leak Bank Customers Data	https://cybersecuritynews.com/icici-bank-data-breach/

3.2 Vulnerabilities and flaws

Σύντομη περιγραφή / Τίτλος	URL
Critical zero-days impact premium WordPress real estate plugins	https://www.bleepingcomputer.com/news/security/critical-zero-days-impact-premium-wordpress-real-estate-plugins/
Cloudflare CDN flaw leaks user location data, even through secure chat apps	https://www.bleepingcomputer.com/news/security/cloudflare-cdn-flaw-leaks-user-location-data-even-through-secure-chat-apps/
Solana private key exfiltration facilitated by illicit npm packages	https://www.scworld.com/brief/solana-private-key-exfiltration-facilitated-by-illicit-npm-packages
Palo Alto Firewalls Found Vulnerable to Secure Boot Bypass and Firmware Exploits	https://thehackernews.com/2025/01/palo-alto-firewalls-found-vulnerable-to.html
phpMyAdmin Vulnerability Let Hackers Trigger XSS Attack With Malicious Tables	https://cybersecuritynews.com/phpmyadmin-triggers-xss-attacks/
PoC Exploit Released For Critical Microsoft Outlook (CVE-2025-21298) Zero-Click RCE Vulnerability	https://cybersecuritynews.com/outlook-zero-click-rce-vulnerability-cve-2025-21298/
Subaru Car Vulnerability Lets Hackers Control Millions of Cars Remotely Using Starlink	https://cybersecuritynews.com/subaru-car-vulnerability-lets-hackers-control-the-millions-of-cars-remotely/

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
High-severity flaw in file archiver 7-Zip requires manual update	https://www.scworld.com/news/high-severity-flaw-in-file-archiver-7-zip-requires-manual-update

Oracle Releases January 2025 Patch to Address 318 Flaws Across Major Products	https://thehackernews.com/2025/01/oracle-releases-january-2025-patch-to.html
Cisco fixes ClamAV vulnerability with available PoC and critical Meeting Management flaw	https://www.helpnetsecurity.com/2025/01/23/cisco-clamav-cve-2025-20128-meeting-management-cve-2025-20156/
Cisco Fixes Critical Vulnerability in Meeting Management	https://www.infosecurity-magazine.com/news/cisco-critical-vulnerability/
SonicWall Urges Immediate Patch for Critical CVE-2025-23006 Flaw Amid Likely Exploitation	https://thehackernews.com/2025/01/sonicwall-urges-immediate-patch-for.html
QNAP fixes six Rsync vulnerabilities in NAS backup, recovery app	https://www.bleepingcomputer.com/news/security/qnap-fixes-six-rsync-vulnerabilities-in-hbs-nas-backup-recovery-app/

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Chinese Cyberspies Target South Korean VPN in Supply Chain Attack	https://www.darkreading.com/threat-intelligence/chinese-cyberspies-target-south-korean-vpn-supply-chain-attack
Two ransomware groups abuse Microsoft's Office 365 platform to gain access to target organizations	https://securityaffairs.com/173328/cyber-crime/ransomware-groups-abuse-microsofts-office-365-platform.html
Major Cybersecurity Vendors' Credentials Found on Dark Web	https://www.infosecurity-magazine.com/news/cybersecurity-vendors-credentials/
CERT-UA warned of scammers impersonating the agency using fake AnyDesk requests	https://securityaffairs.com/173285/hacking/cert-ua-warned-of-scammers-impersonating-the-agency-using-fake-anydesk.html
Russian Ransomware Groups Deploy Email Bombing and Teams Vishing	https://www.infosecurity-magazine.com/news/ransomware-email-bombing-teams/
Beware: Fake CAPTCHA Campaign Spreads Lumma Stealer in Multi-Industry Attacks	https://thehackernews.com/2025/01/beware-fake-captcha-campaign-spreads.html
Juniper enterprise routers backdoored via "magic packet" malware	https://www.helpnetsecurity.com/2025/01/23/juniper-enterprise-routers-backdoor-malware-j-magic/
CISA: Ivanti Vulns Chained Together in Cyberattack Onslaught	https://www.darkreading.com/vulnerabilities-threats/cisa-ivanti-vulns-chained-attacks
New Ransomware Attacking VMware ESXi Hosts Via SSH Tunneling	https://cybersecuritynews.com/ransomware-attacking-vmware-esxi-hosts/
Nnice Ransomware Attacking Windows Systems With Advanced Encryption Techniques	https://cybersecuritynews.com/nnice-ransomware-attacking-windows-systems/

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Web Cache Vulnerability Scanner: Open-source tool for detecting web cache poisoning	https://www.helpnetsecurity.com/2025/01/23/web-cache-vulnerability-scanner-detecting-web-cache-poisoning/
Cybersecurity books on ransomware you shouldn't miss	https://www.helpnetsecurity.com/2025/01/22/ransomware-cybersecurity-books/
New infosec products of the week: January 24, 2025	https://www.helpnetsecurity.com/2025/01/24/new-infosec-products-of-the-week-january-24-2025/

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 Scan your WordPress website,	https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ 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, Research, Collaborate and Act on threat intelligence,	https://cloud.ibm.com/status/security 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, Security Bulletins,	https://support.hpe.com/connect/s/securitybulletinlibrary 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/