Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 02/012024 - 09/01/2025

Contents

1 Common Vulnerabilities and Exposures (CVE)

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-2024-50603	10	Aviatrix Controller	improper neutralization of special elements	before 7.1.4191 and 7.2.x before 7.2.4996	N/A	https://aviatrix.com/ https://docs.aviatrix.com/documentation/latest/network-security/index.html https://docs.aviatrix.com/documentation/latest/release-notices/psirt-advisories/psirt-advisories.html?expand=true#remote-code-execution-vulnerability-in-aviatrix-controllers https://www.securing.pl/en/cve-2024-50603-aviatrix-network-controller-command-injection-vulnerability/
https://nvd.nist.gov/vuln/detail/CVE-2024-10905	10	Sailpoint (IdentityIQ)	Improper Access Control	IdentityIQ 8.4 and all 8.4 patch levels prior to 8.4p2, IdentityIQ 8.3 and all 8.3 patch levels prior to 8.3p5, IdentityIQ 8.2 and all 8.2 patch levels prior to 8.2p8, and all prior versions	N/A	https://www.sailpoint.com/products/identity-security-software/identity-iq https://www.sailpoint.com/security-advisories/identityiq-improper-access-control-vulnerability-cve-2024-10905
https://nvd.nist.gov/vuln/detail/CVE-2024-11635	9.8	WordPress File Upload plugin for WordPress	Remote Code Execution	all versions up to, and including, 4.24.12	N/A	https://wordpress.org/plugins/wp-file-upload/ https://www.wordfence.com/threat-intel/vulnerabilities/id/b5165f60-6515-4a2c-a124-cc88155eaf01?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2023-34060	9.8	VMware Cloud Director Appliance	authentication bypass	N/A	N/A	https://www.vmware.com/products/cloud-infrastructure/cloud-director https://www.vmware.com/security/advisories/VMSA-2023-0026.html
https://nvd.nist.gov/vuln/detail/CVE-2024-12264	9.8	PayU CommercePro Plugin plugin for WordPress	privilege escalation	all versions up to, and including, 3.8.3	N/A	https://wordpress.org/plugins/payu-india/ https://www.wordfence.com/threat-intel/vulnerabilities/id/bf037e4a-2dd7-4296-b86b-635901d2d68f?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-46622	9.8	SecureAge Security Suite	privilege escalation	7.0.x before 7.0.38, 7.1.x before 7.1.11, 8.0.x before 8.0.18, and 8.1.x before 8.1.18	N/A	https://www.secureage.com/products/enterprise-security-software https://www.secureage.com/blog/resolved-escalation-of-privilege
https://nvd.nist.gov/vuln/detail/CVE-2024-54984	9.8	Quectel BG96 BG96MAR02A08M1G	authentication bypass	N/A	N/A	https://www.quectel.com/ https://github.com/haroldfeng/nbiot-va/blob/master/Quecctel_BG96_Message_Auth_Bypass.md

https://nvd.nist.gov/vuln/detail/CVE-2023-33556	9.8	TOTOLink A7100RU	command injection	V7.4cu.2313_B20191024	N/A	https://www.totolink.net/home/menu/newstpl/menu_newstpl/products/id/185.HTML https://github.com/Am1ngl/ttt/tree/main/37
https://nvd.nist.gov/vuln/detail/CVE-2024-54506	9.8	Apple	out-of-bounds access	N/A	macOS Sequoia 15.2	https://el.wikipedia.org/wiki/MacOS https://support.apple.com/en-us/121839
https://nvd.nist.gov/vuln/detail/CVE-2024-45493	9.8	MSA FieldServer Gateway	login bypass	5.0.0 through 6.5.2	7.0.0	https://us.msasafety.com/fieldserver?locale=en https://us.msasafety.com/fieldserver https://us.msasafety.com/security-notices
https://nvd.nist.gov/vuln/detail/CVE-2025-22376	9.8	Perl (Net::OAuth::Client in the Net::Oauth)	not cryptographically strong	before 0.29	N/A	https://metacpan.org/pod/Net::Oauth https://metacpan.org/release/RRWO/Net-OAuth-0.29/changes
https://nvd.nist.gov/vuln/detail/CVE-2024-9140	9.8	Moxa's cellular routers, secure routers, and network security appliances	OS command injection	N/A	N/A	https://www.moxa.com/en/products/industrial-network-infrastructure/cellular-gateways-routers/cellular-routers https://www.moxa.com/en/support/product-support/security-advisory/mpsa-241155-privilege-escalation-and-os-command-injection-vulnerabilities-in-cellular-routers,-secure-routers,-and-netwo
https://nvd.nist.gov/vuln/detail/CVE-2024-12106	9.4	WhatsUp Gold	configure LDAP settings without authentication	before 2024.0.2	N/A	https://www.whatsupgold.com/ https://www.progress.com/network-monitoring
https://nvd.nist.gov/vuln/detail/CVE-2024-41713	9.1	Mitel MiCollab	insufficient input validation	9.8 SP1 FP2 (9.8.1.201)	N/A	https://www.mitel.com/products/micollab-collaboration-software https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029
https://nvd.nist.gov/vuln/detail/CVE-2024-7387	9.1	Openshift/builder (Redhat)	command injection	N/A	N/A	https://docs.openshift.com/container-platform/3.11/creating_images/custom.html https://stuxxn.github.io/advisory/2024/10/02/openshift-build-docker-priv-esc.html
https://nvd.nist.gov/vuln/detail/CVE-2024-53677	9	Apache Struts	bypass file upload checks	from 2.0.0 before 6.4.0	upgrade to version 6.4.0	https://struts.apache.org/ https://security.netapp.com/advisory/ntap-20250103-0005/
https://nvd.nist.gov/vuln/detail/CVE-2025-0282	9	Ivanti Connect Secure	before version 22.7R2.5	before version 22.7R1.2	6.1	https://www.ivanti.com/products/connect-secure-vpn https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283
https://nvd.nist.gov/vuln/detail/CVE-2024-45733	8.8	Splunk Enterprise for Windows	Remote Code Execution	below 9.2.3 and 9.1.6	N/A	https://www.splunk.com/en_us/download.html https://advisory.splunk.com/advisories/SVD-2024-1003
https://nvd.nist.gov/vuln/detail/CVE-2024-36985	8.8	Splunk Enterprise	Remote Code Execution	below 9.2.2, 9.1.5, and 9.0.10	N/A	https://www.splunk.com/en_us/products/splunk-enterprise.html https://advisory.splunk.com/advisories/SVD-2024-0705
https://nvd.nist.gov/vuln/detail/CVE-2024-12692	8.8	Google Chrome	exploit heap corruption	prior to 131.0.6778.204	N/A	https://www.google.com/chrome https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-desktop_18.html

https://nvd.nist.gov/vuln/detail/CVE-2024-10957	8.8	UpdraftPlus: WP Backup & Migration Plugin plugin for WordPress	PHP Object Injection	all versions from 1.23.8 to 1.24.11	N/A	https://wordpress.org/plugins/updraftplus/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4729ed37-96b2-4717-8a72-89b9a21ec058?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-12829	8.8	Arista NG Firewall ExecManagerImpl	Remote Code Execution	N/A	N/A	https://edge.arista.com/ng-firewall/ https://www.zerodayinitiative.com/advisories/ZDI-24-1717/
https://nvd.nist.gov/vuln/detail/CVE-2024-40702	8.2	IBM Cognos Controller	improper certificate validation	IBM Cognos Controller 11.0.0 through 11.0.1 and IBM Controller 11.1.0	N/A	https://www.ibm.com/products/controller https://www.ibm.com/support/pages/node/7179163
https://nvd.nist.gov/vuln/detail/CVE-2025-22395	8.2	Dell Update Package Framework	prior to 22.01.02	Local Privilege Escalation	N/A	https://www.dell.com/support/kbdoc/en-us/000127316/dell-update-package https://www.dell.com/support/kbdoc/en-us/000269079/dsa-2025-034-security-update-for-dell-update-package-dup-framework-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2024-10012	7.8	Progress Telerik UI for WPF versions	unsafe deserializatio n vulnerability	prior to 2024 Q4 (2024.4.1111)	N/A	https://www.telerik.com/ https://docs.telerik.com/devtools/wpf/knowledge-base/kb-security-unsafe-deserialization-cve-2024-10012
https://nvd.nist.gov/vuln/detail/CVE-2024-8811	7.8	WinZip	Mark-of-the-Web Bypass Vulnerability	N/A	N/A	https://www.winzip.com/en/ https://www.zerodayinitiative.com/advisories/ZDI-24-1234/
https://nvd.nist.gov/vuln/detail/CVE-2025-21102	7.5	Dell VxRail	Plaintext Storage of a Password	7.0.000 through 7.0.532	N/A	https://www.dell.com/en-us/dt/converged-infrastructure/vxrail/index.htm#scroll=off&tab0=0&tab1=0 https://www.dell.com/support/kbdoc/en-us/000269793/dsa-2025-027-security-update-for-dell-vxrail-for-multiple-vulnerabilities?ref=emcadvisory_000269793_High_null
https://nvd.nist.gov/vuln/detail/CVE-2024-21259	7.5	Oracle VM VirtualBox	takeover of Oracle VM VirtualBox	Prior to 7.0.22 and prior to 7.1.2	N/A	https://www.virtualbox.org/ https://www.oracle.com/security-alerts/cpuoct2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-48457	7.5	Netis Routers	remote attacker to obtain sensitive information	Multiple products	N/A	https://www.netis-systems.com/products/N6.html https://github.com/users/h00die-gr3y/projects/1/views/1
https://nvd.nist.gov/vuln/detail/CVE-2024-28197	7.5	Zitadel	Bypassing MFA	N/A	2.46.0, 2.45.1, and 2.44.3	https://zitadel.com/ https://github.com/zitadel/zitadel/security/advisories/GHSA-mq4x-r2w3-j7mr
https://nvd.nist.gov/vuln/detail/CVE-2024-53916	7.5	OpenStack Neutron	incorrect ID during policy enforcement	23 before 23.2.1, 24 before 24.0.2, and 25 before 25.0.1	N/A	https://wiki.openstack.org/wiki/Neutron https://security.openstack.org/ossa/OSSA-2024-005.html
https://nvd.nist.gov/vuln/detail/CVE-2024-8474	7.5	OpenVPN Connect	unauthorized actor can use to decrypt the VPN traffic	before version 3.5.0	N/A	https://openvpn.net/client/client-connect-vpn-for-windows/ https://openvpn.net/connect-docs/android-release-notes.html

https://nvd.nist.gov/vuln/detail/CVE-2024-45802	7.5	Squid open source caching proxy	Denial of Service	N/A	6.1	https://www.squid-cache.org/ https://security.netapp.com/advisory/ntap-20250103-0004/
https://nvd.nist.gov/vuln/detail/CVE-2024-41767	7.3	IBM Engineering Lifecycle Optimization - Publishing	SQL injection	7.0.2 and 7.0.3	N/A	https://www.ibm.com/docs/en/engineering-lifecycle-management-suite/lifecycle-optimization-publishing/7.0.2?topic=overview https://www.ibm.com/support/pages/node/7180199
https://nvd.nist.gov/vuln/detail/CVE-2024-54007	7.2	501 Wireless Client Bridge	Remote Command Injection	N/A	N/A	https://www.hpe.com/psnow/doc/a00093384enw https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04763en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/CVE-2024-12430	7	AC500 V3 (ABB)	command execution	firmware version earlier than 3.8.0	N/A	https://new.abb.com/plc/programmable-logic-controllers-plcs/ac500 https://search.abb.com/library/Download.aspx?DocumentID=3ADR011377&LanguageCode=en&DocumentPartId=&Action=Launch

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2024-41713 Mitel MiCollab Path Traversal Vulnerability CVE-2024-55550 Mitel MiCollab Path Traversal Vulnerability CVE-2020-2883 Oracle WebLogic Server Unspecified Vulnerability CVE-2025-0282 Ivanti Connect Secure Vulnerability	https://www.cisa.gov/news-events/alerts/2025/01/07/cisa-adds-three-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2025/01/08/cisa-adds-one-vulnerability-kev-catalog
CISA Releases Industrial Control Systems Advisories	ICSA-25-007-01 ABB ASPECT-Enterprise, NEXUS, and MATRIX Series Products ICSA-25-007-02 Nedap Librix Ecoreader	https://www.cisa.gov/news-events/alerts/2025/01/07/cisa-releases-two-industrial-control-systems-advisories
Ivanti Releases Security Updates for Connect Secure, Policy Secure, and ZTA Gateways	Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-0282, CVE-2025-0283)	https://www.cisa.gov/news-events/alerts/2025/01/08/ivanti-releases-security-updates-connect-secure-policy-secure-and-zta-gateways

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
Over 4,000 backdoors hijacked by registering expired domains	https://www.bleepingcomputer.com/news/security/over-4-000-backdoors-hijacked-by-registering-expired-domains/
ESET urges migration from Windows 10 ahead of support deadline	https://www.scworld.com/brief/eset-urges-migration-from-windows-10-ahead-of-support-deadline
US adds Tencent to the list of companies supporting Chinese military	https://securityaffairs.com/172765/security/us-adds-tencent-list-of-companies-supporting-chinese-military.html
Government Launches £1.9m Initiative to Boost UK's Cyber Resilience	https://www.infosecurity-magazine.com/news/government-19m-boost-uks-cyber/
32 Million Windows 10 Devices At Risk As Microsoft Ends Support	https://cybersecuritynews.com/32-million-windows-10-devices-at-risk/
Nvidia Unveils Digits, $3,000 Personal AI Supercomputer	https://cybersecuritynews.com/nvidia-personal-ai-supercomputer/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Russian ISP confirms Ukrainian hackers "destroyed" its network	https://www.bleepingcomputer.com/news/security/russian-isp-confirms-ukrainian-hackers-destroyed-its-network/
Casio Data Breach Ransomware Attack Compromised 8,500 Individuals	https://dailysecurityreview.com/security-spotlight/casio-data-breach-ransomware-attack-compromised-8500-individuals/
PowerSchool Hack Exposes Sensitive Data of Students and Teachers in K-12 Districts	https://dailysecurityreview.com/security-spotlight/powerschool-hack-exposes-sensitive-data-of-students-and-teachers-in-k-12-districts/
Thousands of credit cards stolen in Green Bay Packers store breach	https://www.bleepingcomputer.com/news/security/thousands-of-credit-cards-stolen-in-green-bay-packers-store-breach/
UN aviation agency confirms recruitment database security breach	https://www.bleepingcomputer.com/news/security/un-aviation-agency-confirms-recruitment-database-security-breach/
Threat actors breached the Argentina's airport security police (PSA) payroll	https://securityaffairs.com/172776/uncategorized/argentinas-airport-security-police-psa-payroll-hacked.html
City Bank Data Breach: Client Financial Statements Sold on Underground Forums	https://dailysecurityreview.com/security-spotlight/city-bank-data-breach/
Gravy Analytics Hacked – Attackers Allegedly Claiming 17TB Data Stolen	https://cybersecuritynews.com/hackers-allegedly-stolen-17tb-of-data/
Nikki-Universal Cyber Attack – Hackers Claim 761.8 GB of Data Stolen	https://cybersecuritynews.com/nikki-universal-cyber-attack/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Critical RCE Flaw in GFI KerioControl Allows Remote Code Execution via CRLF Injection	https://thehackernews.com/2025/01/critical-rce-flaw-in-gfi-keriocontrol.html
Critical Ivanti Zero-Day Exploited in the Wild	https://www.infosecurity-magazine.com/news/critical-ivanti-zeroday-exploited/
SonicWall warns of an exploitable SonicOS vulnerability	https://securityaffairs.com/172823/security/sonicwall-sonicos-authentication-bypass-flaw.html
Unpatched critical flaws impact Fancy Product Designer WordPress plugin	https://www.bleepingcomputer.com/news/security/unpatched-critical-flaws-impact-fancy-product-designer-wordpress-plugin/
Gayfemboy Botnet targets Four-Faith router vulnerability	https://securityaffairs.com/172805/malware/gayfemboy-mirai-botnet-four-faith-flaw.html
Critical Vulnerabilities in Moxa Routers Allow Root Privilege Escalation	https://hackread.com/moxa-reports-critical-industrial-router-vulnerabilities/

Netis routers vulnerable to chained authentication bypass, RCE flaws	https://www.scworld.com/news/netis-routers-vulnerable-to-chained-authentication-bypass-rce-flaws
LDAP Nightmare: Zero-Click Exploit CVE-2024–49112 Rocks Windows Servers — Patch Now!	https://medium.com/@scottbolen/ldap-nightmare-zero-click-exploit-cve-2024-49112-rocks-windows-servers-patch-now-d8d1170140b1
Palo Alto Networks Expedition Tool Vulnerability Exposes Firewall Credentials	https://cybersecuritynews.com/palo-alto-networks-expedition-tool-vulnerability/
Critical MediaTek Processor RCE Vulnerability Impacts Millions of Devices	https://cybersecuritynews.com/mediatek-processor-vulnerabilities/
Redis Server Vulnerabilities Let Attackers Execute Remote Code	https://cybersecuritynews.com/redis-server-vulnerabilities/
ASUS Routers Vulnerabilities Allows Arbitrary Code Execution	https://cybersecuritynews.com/asus-router-vulnerabilities/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Hackers take Pride in exploiting Four-Faith zero day	https://www.scworld.com/news/hackers-take-pride-in-exploiting-four-faith-zero-day
Millions of Email Servers Exposed Due to Missing TLS Encryption	https://hackread.com/millions-email-servers-exposed-missing-tls-encryption/
Ransomware Targeting Infrastructure Hits Telecom Namibia	https://www.darkreading.com/cyberattacks-data-breaches/ransomware-targeting-infrastructure-telecom-namibia
PhishWP Plug-in Hijacks WordPress E-Commerce Checkouts	https://www.darkreading.com/threat-intelligence/phishwp-plugin-hijacks-wordpress-e-commerce-checkouts
48,000+ Vulnerable SonicWall Devices Under Attack From Akira And Fog Ransomware	https://cybersecuritynews.com/48000-vulnerable-sonicwall-devices/
Windows 11 BitLocker Encryption Bypassed To Extract Volume Encryption Keys	https://cybersecuritynews.com/windows-11-bitlocker-encryption-bypassed/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Sara: Open-source RouterOS security inspector	https://www.helpnetsecurity.com/2025/01/09/sara-open-source-routeros-security-inspector/
20 Best Threat Hunting Tools – 2025	https://cybersecuritynews.com/threat-hunting-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/