Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/02/2025 - 21/02/2025

Contents

1 Common Vulnerabilities and Exposures (CVEs) 2

2 CISA/CERT-EU Alerts & Advisories 5

3 News 5

3.1 Breaches / Compromised / Hacked 6

3.2 Vulnerabilities / Flaws / Zero-day 6

3.3 Patches / Updates / Fixes 7

3.4 Potential threats / Threat intelligence 7

3.5 Guides / Tools 8

4 References 9

5 Annex – Websites with vendor specific vulnerabilities 10

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-2022-3682	9.9	MicroSCADA X SDM600 (Hitachi Energy)	Arbitrary code Executing	Multiple versions	N/A	https://www.hitachienergy.com/products-and-solutions/scada/microscada-x/sdm600 https://search.abb.com/library/Download.aspx?DocumentID=8DBD000138&LanguageCode=en&DocumentPartId=&Action=Launch
https://nvd.nist.gov/vuln/detail/CVE-2019-1003029	9.9	Jenkins Script Security Plugin	sandbox bypass	1.53 and earlier	N/A	https://plugins.jenkins.io/script-security/ https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1336%20
https://nvd.nist.gov/vuln/detail/CVE-2025-22467	9.9	Ivanti Connect Secure	stack-based buffer overflow	before version 22.7R2.6	N/A	https://www.ivanti.com/products/connect-secure-vpn https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs
https://nvd.nist.gov/vuln/detail/CVE-2023-27232	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/32
https://nvd.nist.gov/vuln/detail/CVE-2025-1044	9.8	Logsign Unified SecOps Platform	Authentication Bypass	N/A	N/A	https://www.logsign.com/ https://support.logsign.net/hc/en-us/articles/22076844908946-18-10-2024-Version-6-4-32-Release-Notes https://www.zerodayinitiative.com/advisories/ZDI-25-085/
https://nvd.nist.gov/vuln/detail/CVE-2022-36983	9.8	Ivanti Avalanche	Authentication Bypass	N/A	N/A	https://www.ivanti.com/products/avalanche https://download.wavelink.com/Files/avalanche_v6.3.4_release_notes.txt https://www.zerodayinitiative.com/advisories/ZDI-22-788/
https://nvd.nist.gov/vuln/detail/CVE-2025-23006	9.8	SMA1000 Appliance Management Console (AMC)	arbitrary OS commands	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-2022-26138	9.8	Atlassian Questions For Confluence app for Confluence Server and Data Center	hardcoded password	2.7.34, 2.7.35, and 3.0.2	N/A	https://www.atlassian.com/software/confluence/download-archives https://confluence.atlassian.com/doc/confluence-security-advisory-2022-07-20-1142446709.html https://jira.atlassian.com/browse/CONFSERVER-79483
https://nvd.nist.gov/vuln/detail/CVE-2023-26800	9.8	Ruijie Networks RG-EW1200 Wireless Routers	command injetion	EW_3.0(1)B11P204	N/A	https://reyee.ruijie.com/en-global/products/home-wifi/wifi-router/wifi5-router/rg-ew1200 https://github.com/winmt/my-vuls/tree/main/RG-EW1200
https://nvd.nist.gov/vuln/detail/CVE-2025-21547	9.1	Oracle Hospitality OPERA 5	unauthorized access to critical data	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-2025-0108	9.1	Palo Alto Networks PAN-OS software	authentication bypass	N/A	N/A	https://docs.paloaltonetworks.com/pan-os https://security.paloaltonetworks.com/CVE-2025-0108
https://nvd.nist.gov/vuln/detail/CVE-2024-47908	9.1	Ivanti CSA	OS command injection	before version 5.0.5	N/A	https://help.ivanti.com/ld/help/en_US/LDMS/10.0/Windows/csa-h-help.htm https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Services-Application-CSA-CVE-2024-47908-CVE-2024-11771
https://nvd.nist.gov/vuln/detail/CVE-2021-44967	8.8	LimeSurvey	Remote Code Execution	5.2.4	N/A	https://www.limesurvey.org/ https://www.limesurvey.org/manual/Plugins_-_advanced
https://nvd.nist.gov/vuln/detail/CVE-2023-27042	8.8	Tenda AX3	Buffer Overflow	V16.03.12.11	N/A	https://www.tendacn.com/product/overview/no-ax3.html https://github.com/hujianjie123/vuln/blob/main/Tenda/SetFirewallCfg/readme.md
https://nvd.nist.gov/vuln/detail/CVE-2023-37931	8.6	FortiVoice Entreprise	improper neutralization of special elements	7.0.0 through 7.0.1 and before 6.4.8	N/A	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiVoiceEnterprise.pdf https://fortiguard.com/psirt/FG-IR-23-220

https://nvd.nist.gov/vuln/detail/CVE-2023-27284	8.4	IBM Aspera Cargo 4.2.5 and IBM Aspera Connect	buffer overflow	4.2.5	N/A	https://www.ibm.com/docs/en/aspera-cargo https://www.ibm.com/support/pages/node/6966588
https://nvd.nist.gov/vuln/detail/CVE-2024-47572	8.3	Fortinet FortiSOAR	improper neutralization	7.2.1 through 7.4.1	N/A	https://www.fortinet.com/products/fortisoar https://fortiguard.fortinet.com/psirt/FG-IR-24-210
https://nvd.nist.gov/vuln/detail/CVE-2024-47571	7.9	Fortinet FortiManager	attacker may gain improper access to FortiGate via valid credentials	6.4.12 through 7.4.0	N/A	https://www.fortinet.com/products/management/fortimanager https://fortiguard.fortinet.com/psirt/FG-IR-24-239
https://nvd.nist.gov/vuln/detail/CVE-2025-21532	7.8	Oracle Analytics Desktop	low privileged attacker with logon may compromise system	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-2025-1492	7.8	Wireshark	denial of service via packet injection	4.4.0 to 4.4.3 and 4.2.0 to 4.2.10	N/A	https://www.wireshark.org/ https://www.wireshark.org/security/wnpa-sec-2025-01.html
https://nvd.nist.gov/vuln/detail/CVE-2024-23106	7.7	FortiClientEMS	improper restriction of excessive authentication attempts	7.2.0 through 7.2.4 and before 7.0.10	N/A	https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/35450/forticlient-ems-endpoint-management-server https://fortiguard.fortinet.com/psirt/FG-IR-23-476
https://nvd.nist.gov/vuln/detail/CVE-2025-21549	7.5	Oracle WebLogic Server	unauthorized activity may cause a hang or frequently repeatable crash	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-2025-25901	7.5	TP-Link TL-WR841ND V11	Buffer Overflow	V11	N/A	https://www.tp-link.com/us/home-networking/wifi-router/tl-wr841nd/ https://github.com/2664521593/mycve/blob/main/TP-Link/BOF_in_TP-Link_TL-WR841ND-V11_5.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-49781	7.1	IBM OpenPages	XML external entity injection (XXE)	8.3 and 9.0	N/A	https://www.ibm.com/products/openpages https://www.ibm.com/support/pages/node/7183541

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Industrial Control Systems Advisories	ICSA-24-191-01 Delta Electronics CNCSoft-G2 (Update A) ICSA-25-035-02 Rockwell Automation GuardLogix 5380 and 5580 (Update A) ICSA-25-051-01 ABB ASPECT-Enterprise, NEXUS, and MATRIX Series ICSA-25-051-02 ABB FLXEON Controllers ICSA-25-051-04 Siemens SiPass Integrated ICSA-25-051-05 Rapid Response Monitoring My Security Account App ICSA-25-051-06 Elseta Vinci Protocol Analyzer ICSA-24-291-03 Mitsubishi Electric CNC Series (Update A) ICSMA-25-051-01 Medixant RadiAnt DICOM Viewer	https://www.cisa.gov/news-events/alerts/2025/02/18/cisa-releases-two-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2025/02/20/cisa-releases-seven-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2025-0108 Palo Alto PAN-OS Authentication Bypass Vulnerability CVE-2024-53704 SonicWall SonicOS SSLVPN Improper Authentication Vulnerability CVE-2025-23209 Craft CMS Code Injection Vulnerability CVE-2025-0111 Palo Alto Networks PAN-OS File Read Vulnerability	https://www.cisa.gov/news-events/alerts/2025/02/18/cisa-adds-two-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2025/02/20/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA and Partners Release Advisory on Ghost (Cring) Ransomware	#StopRansomware: Ghost (Cring) Ransomware.	https://www.cisa.gov/news-events/alerts/2025/02/19/cisa-and-partners-release-advisory-ghost-cring-ransomware
Vulnerability Summary for the Week of February 10, 2025	Common Vulnerabilities and Exposures (CVE)	https://www.cisa.gov/news-events/bulletins/sb25-049

3 News

Σύντομη περιγραφή / Τίτλος	URL
Hundreds of US Military and Defense Credentials Compromised	https://www.infosecurity-magazine.com/news/us-military-defense-credentials/

Cyber Threat Actors Leveraging Exploits To Attack Financial Sector With Advanced Malware	https://cybersecuritynews.com/threat-actors-attack-financial-sector-with-advanced-malware/
Chinese hackers use custom malware to spy on US telecom networks	https://www.bleepingcomputer.com/news/security/salt-typhoon-uses-jumbledpath-malware-to-spy-on-us-telecom-networks/
Cisco Confirms Salt Typhoon Exploited CVE-2018-0171 to Target U.S. Telecom Networks	https://thehackernews.com/2025/02/cisco-confirms-salt-typhoon-exploited.html
Microsoft's Quantum Chip Breakthrough Accelerates Threat to Encryption Protocols	https://www.infosecurity-magazine.com/news/microsoft-quantum-chip-encryption/
Free SOC Webinar – Better SOC with Interactive Malware Sandbox, Practical Use Cases 2025	https://cybersecuritynews.com/webinar-on-soc/

3.1 Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Fintech giant Finastra notifies victims of October data breach	https://www.bleepingcomputer.com/news/security/fintech-giant-finastra-notifies-victims-of-october-data-breach/
Over 330 Million Credentials Compromised by Infostealers	https://www.infosecurity-magazine.com/news/330-million-credentials/
Clinical Research Firm Exposes 1.6 Million US Medical Survey Records	https://hackread.com/clinical-research-firm-expose-us-medical-survey-records/
Yahoo Data Leak – Hackers Allegedly Advertised 602,000 Email Accounts	https://cybersecuritynews.com/yahoo-data-leak/

3.2 Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
OpenSSH bugs allows Man-in-the-Middle and DoS Attacks	https://securityaffairs.com/174384/security/openssh-vulnerabilities-mitm-dos.html
SPAWNCHIMERA Malware Exploiting Ivanti Buffer Overflow Vulnerability By Applying A Fix	https://cybersecuritynews.com/spawnchimera-malware-exploiting-ivanti-buffer-overflow-flaw/
Ivanti Endpoint Manager Vulnerabilities Proof-of-Concept (PoC) Exploit Released	https://cybersecuritynews.com/ivanti-endpoint-manager-vulnerabilities-proof-of-concept-poc-exploit-released/
Google Released PoC Exploit For Palo Alto Firewall Command Injection Vulnerability	https://cybersecuritynews.com/google-released-poc-exploit-for-palo-alto-firewall/
China-Linked Attackers Exploit Check Point Flaw to Deploy ShadowPad and Ransomware	https://thehackernews.com/2025/02/chinese-linked-attackers-exploit-check.html
Hackers Chain Exploits of Three Palo Alto Networks Firewall Flaws	https://www.infosecurity-magazine.com/news/hackers-chain-exploits-three-palo/

Symantec Diagnostic Tool Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/symantec-diagnostic-tool-vulnerability/
Critical Microsoft Bing Vulnerability Let Attackers Execute Code Remotely	https://cybersecuritynews.com/microsoft-bing-remote-code-execution-vulnerability/
90,000 WordPress Sites Vulnerable to Local File Inclusion Attacks	https://cybersecuritynews.com/90000-wordpress-sites-vulnerable/
Critical Apache Ignite Vulnerability Let Attackers Execute Remote Code	https://cybersecuritynews.com/critical-apache-ignite-vulnerabilitycve-2024-52577/

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Xerox Versalink printers are vulnerable to pass-back attacks. Rapid7 discovers LDAP & SMB flaws (CVE-2024-12510 & CVE-2024-12511). Update firmware now!	https://hackread.com/xerox-versalink-printers-vulnerabilities-hackers-steal-credentials/
Juniper Networks fixed a critical flaw in Session Smart Routers	https://securityaffairs.com/174365/security/juniper-networks-fixed-a-critical-flaw-in-session-smart-routers.html
Microsoft fixed actively exploited flaw in Power Pages	https://securityaffairs.com/174430/security/microsoft-fixed-actively-exploited-flaw-in-power-pages.html
Citrix addressed NetScaler console privilege escalation flaw	https://securityaffairs.com/174425/security/citrix-addressed-netscaler-console-privilege-escalation-flaw.html
Atlassian fixed critical flaws in Confluence and Crowd	https://securityaffairs.com/174474/security/atlassian-fixed-critical-flaws-in-confluence-and-crowd.html
Firefox 135.0.1 Released with Fix for High-Severity Memory Safety Vulnerabilities	https://cybersecuritynews.com/firefox-135-0-1-released-with-fix/

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Russian phishing campaigns exploit Signal's device-linking feature	https://www.bleepingcomputer.com/news/security/russian-phishing-campaigns-exploit-signals-device-linking-feature/
Attackers are chaining flaws to breach Palo Alto Networks firewalls	https://www.helpnetsecurity.com/2025/02/19/palo-alto-networks-firewalls-cve-2025-0108-cve-2024-9474-cve-2025-0111/
Pegasus Spyware Used Widely to Target Individuals in Private Industry & Finance Sectors	https://cybersecuritynews.com/pegasus-spyware-used-widely-to-target-individuals/
Windows Wi-Fi Password Stealer Malware Found Hosted on GitHub	https://cybersecuritynews.com/windows-wi-fi-password-stealer-github/
NailaoLocker ransomware targets EU healthcare-related entities	https://securityaffairs.com/174440/malware/nailaolocker-ransomware-targets-eu-healthcare-related-entities.html
Revamped darcula phishing kit impersonates sites with just a link	https://www.scworld.com/news/new-darcula-phishing-kit-can-impersonate-any-site-with-just-a-link

Ghost Ransomware Compromised Organisations Across 70+ Countries – CISA & FBI Warns	https://cybersecuritynews.com/ghost-ransomware-compromised-70-organisations/

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Kunai: Open-source threat hunting tool for Linux	https://www.helpnetsecurity.com/2025/02/19/kunai-open-source-threat-hunting-tool-for-linux/
Integrating LLMs into security operations using Wazuh	https://www.bleepingcomputer.com/news/security/integrating-llms-into-security-operations-using-wazuh/
PRevent: Open-source tool to detect malicious code in pull requests	https://www.helpnetsecurity.com/2025/02/20/prevent-open-source-tool-to-detect-malicious-code-in-pull-requests/
New infosec products of the week: February 21, 2025	https://www.helpnetsecurity.com/2025/02/21/new-infosec-products-of-the-week-february-21-2025/
NSA Added New Features to Supercharge Ghidra 11.3	https://cybersecuritynews.com/ghidra-11-3-new-features/

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/