Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 28/03/2025 - 01/04/2025

Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-2328	8,8	Contact Form 7 plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	the 'dnd_remove_uploaded_files' function in all versions up to, and including, 1.3.8.7	
https://nvd.nist.gov/vuln/detail/CVE-2025-24381	8,8	Dell Unity	URL Redirection to Untrusted Site ('Open Redirect')	version(s) 5.4 and prior	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-21384	8,3	Microsoft Azure	Protection Mechanism Failure	Microsoft Azure Health Bot	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21384
https://nvd.nist.gov/vuln/detail/CVE-2025-26683	8,1	Azure	Improper Authorization	Azure Playwright	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26683

https://nvd.nist.gov/vuln/detail/CVE-2025-24386	7,8	Dell Unity	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	version(s) 5.4 and prior	https://www.dell.com/support/kbdoc/en-us/000300090/dsa-2025-116-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2023-0881	7,5	tcp port 22	Improper Input Validation	Running DDoS on tcp port 22 will trigger a kernel crash	https://bugs.launchpad.net/ubuntu/+source/linux-bluefield/+bug/2006397

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Malware Analysis Report on RESURGE Malware Associated with Ivanti Connect Secure	**CVE-2025-0282**	https://www.cisa.gov/news-events/alerts/2025/03/28/cisa-releases-malware-analysis-report-resurge-malware-associated-ivanti-connect-secure
CISA Adds One Known Exploited Vulnerability to Catalog	**CVE-2024-20439**	https://www.cisa.gov/news-events/alerts/2025/03/31/cisa-adds-one-known-exploited-vulnerability-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
Lazarus Group is No Longer Consider a Single APT Group, But Collection of Many Sub Groups	https://cybersecuritynews.com/lazarus-group-is-no-longer-consider-a-single-apt-group/
New Ubuntu Security Bypasses Allow Attackers to Exploit Kernel Vulnerabilities	https://cybersecuritynews.com/ubuntu-security-bypasses/
Russian Hackers Using Russia-Based Bulletproof Network to Switch Network Infrastructure	https://cybersecuritynews.com/russian-hackers-using-russia-based-bulletproof-network/
Threats Actors Hide Malware in WordPress Websites to Execute Code Remotely	https://cybersecuritynews.com/threats-actors-hide-malware-in-wordpress-websites/
Russian Hackers Mimic as CIA to Steal Ukraine Defense Intelligence Data	https://cybersecuritynews.com/russian-hackers-mimic-as-cia/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Daisy Cloud Hacker Group Exposed 30K Login Credentials Across a Wide Range of Services	https://cybersecuritynews.com/daisy-cloud-hacker-group-exposed-30k-login-credentials/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Cannon Printer Vulnerability Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/cannon-printer-vulnerability-arbitrary-code/
Multiple Dell Unity Vulnerabilities Let Attackers Compromise Affected System	https://cybersecuritynews.com/multiple-dell-unity-vulnerabilities/
Apache Tomcat Vulnerability (CVE-2025-24813) Exploited to Execute Code on Servers	https://cybersecuritynews.com/apache-tomcat-vulnerability-exploited/
Hackers Employ New ClickFix Captcha Technique to Deliver Ransomware	https://cybersecuritynews.com/clickfix-captcha-technique-ransomware/
Windows Server 2025 Security Update Freezes Remote Desktop Sessions Connection	https://cybersecuritynews.com/windows-server-2025-security-update/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Hackers Leveraging DNS MX Records To Dynamically Create Fake Logins Mimic as 100+ Brands	https://cybersecuritynews.com/hackers-leveraging-dns-mx-records-to-dynamically-create-fake-logins/
ClickFix Captcha – A Creative Technique That Allow Attackers Deliver Malware and Ransomware on Windows	https://cybersecuritynews.com/clickfix-captcha-a-creative-technique/
Crocodilus – A New Android Malware Remotely Control Your Android Devices	https://cybersecuritynews.com/crocodilus/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Mozilla Releases Urgent Patch for Windows Users Following Exploited Chrome 0-Day	https://cybersecuritynews.com/mozilla-releases-urgent-patch-for-windows-users/
Tor Browser 14.0.8 Released Emergency Update for Windows Users	https://cybersecuritynews.com/tor-browser-14-0-8-released-emergency-update/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
20 Best Remote Monitoring Tools – 2025	https://cybersecuritynews.com/best-remote-monitoring-tools/

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.

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/