Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 06/12/2024 - 10/12/2024

Contents

1 Common Vulnerabilities and Exposures (CVE)

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-2024-37143	**10**	Dell PowerFlex appliance	Improper Link Resolution	Multiple versions	N/A	https://www.dell.com/en-us/shop/powerflex/sf/powerflex https://www.dell.com/support/kbdoc/en-us/000258342/dsa-2024-405-security-update-for-dell-products-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-53822	**10**	Genetech Pie Register Premium.	Unrestricted Upload of File with Dangerous Type	from n/a before 3.8.3.3	N/A	https://www.genetechsolutions.com/product/pie-register.html https://patchstack.com/database/wordpress/plugin/pie-register-premium/vulnerability/wordpress-pie-register-premium-plugin-3-8-3-3-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-12209	**9.8**	WP Umbrella: Update Backup Restore & Monitoring plugin for WordPress	PHP Remote File Inclusion	all versions up to, and including, 2.17.0	N/A	https://wordpress.org/plugins/wp-health/ https://www.wordfence.com/threat-intel/vulnerabilities/id/c74ce3e8-cab9-4cc6-a1ad-1e51f7268474?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-52324	**9.8**	Ruijie Reyee OS	Use of Inherently Dangerous Function	2.206.x up to but not including 2.320.x	N/A	https://reyee.ruijie.com/en-global/ https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-01
https://nvd.nist.gov/vuln/detail/CVE-2024-54750	**9.8**	Ubiquiti U6-LR	Use of Hard-coded Credentials	6.6.65	N/A	https://store.ui.com/us/en/products/u6-lr https://colorful-meadow-5b9.notion.site/U6-LR_HardCode_vuln-14bc216a1c30806487ebdda3bb984e91?pvs=4
https://nvd.nist.gov/vuln/detail/CVE-2024-54136	**9.8**	ClipBucket V5	Deserialization of Untrusted Data	Version 5.5.1 Revision 199 and below	N/A	https://github.com/MacWarrior/clipbucket-v5 https://github.com/MacWarrior/clipbucket-v5/security/advisories/GHSA-vxvf-5cmq-5f78
https://nvd.nist.gov/vuln/detail/CVE-2024-53908	**9.8**	Django CMS	Improper Neutralization of Special Elements	5.1 before 5.1.4, 5.0 before 5.0.10, and 4.2 before 4.2.17	N/A	https://www.djangoproject.com/ https://docs.djangoproject.com/en/dev/releases/security/ https://groups.google.com/g/django-announce https://www.openwall.com/lists/oss-security/2024/12/04/3

https://nvd.nist.gov/vuln/detail/CVE-2024-37863	9.8	Open Robotics Robotic Operating System 2 (ROS2) and Nav2	Classic Buffer Overflow	N/A	N/A	https://ros.org/ https://github.com/GoesM/ROS-CVE-CNVDs https://github.com/ros-navigation/navigation2/issues/4005 https://github.com/ros-navigation/navigation2/issues/4337
https://nvd.nist.gov/vuln/detail/CVE-2024-55560	9.8	MailCleaner	default values of ssh_host_dsa_key, ssh_host_rsa_key, and ssh_host_ed25519_key	before 28d913e	N/A	https://www.mailcleaner.net/ https://github.com/MailCleaner/MailCleaner/commit/28d913eaa044b689eb114f72ebe92d48cb4aaca7 https://github.com/MailCleaner/MailCleaner/wiki/Watchdogs#host_keys https://www.mailcleaner.net/infobox/mc-info-box.php
https://nvd.nist.gov/vuln/detail/CVE-2024-47578	9.1	Adobe Document Service	Server-Side Request Forgery (SSRF)	N/A	N/A	https://developer.adobe.com/document-services/docs/overview/ https://community.sap.com/t5/technology-blogs-by-members/sap-security-patch-day-december-2024/ba-p/13959582
https://nvd.nist.gov/vuln/detail/CVE-2024-51815	9	WP Sharks s2Member Pro	Code Injection	from n/a through 241114	N/A	https://wordpress.org/plugins/s2member/ https://patchstack.com/database/wordpress/plugin/s2member/vulnerability/wordpress-s2member-excellent-for-all-kinds-of-memberships-content-restriction-paywalls-member-access-subscriptions-plugin-241114-remote-code-execution-rce-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10773	9	SICK sensors	Hidden Functionality	N/A	N/A	https://www.sick.com/be/en/catalog/products/machine-vision-and-identification/machine-vision/inspectorp61x/c/g555810 https://www.sick.com/.well-known/csaf/white/2024/sca-2024-0006.pdf https://www.cisa.gov/resources-tools/resources/ics-recommended-practices
https://nvd.nist.gov/vuln/detail/CVE-2024-55579	8.8	Qlik Sense Enterprise for Windows	execution of arbitrary EXE files	N/A	November 2024 IR, May 2024 Patch 10, February 2024 Patch 14, November 2023 Patch 16, August 2023 Patch 16, May 2023 Patch 18, and February 2023 Patch 15	https://insightsoftware.com/vizlib/ https://community.qlik.com/t5/Official-Support-Articles/High-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows-CVEs/tac-p/2496004
https://nvd.nist.gov/vuln/detail/CVE-2024-11323	8.8	AI Quiz | Quiz Maker plugin for WordPress	Missing Authorization	all versions up to, and including, 1.1	N/A	https://wordpress.org/plugins/quiz-maker/ https://www.wordfence.com/threat-intel/vulnerabilities/id/53591a3b-8a99-40e2-8145-1d7785bcbab4?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2024-53808	8.5	Basix NEX-Forms – Ultimate Form Builder	SQL Injection	from n/a through 8.7.8	N/A	https://wordpress.org/plugins/nex-forms-express-wp-form-builder/ https://patchstack.com/database/wordpress/plugin/nex-forms-express-wp-form-builder/vulnerability/wordpress-nex-forms-plugin-8-7-8-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-54198	8.5	SAP NetWeaver Application Server ABAP	Improper Control of Dynamically-Identified Variables	N/A	N/A	https://help.sap.com/doc/saphelp_nw75/7.5.5/en-US/d0/ec44e837174b0da80d558c1c142cba/content.htm https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
https://nvd.nist.gov/vuln/detail/CVE-2024-21571	8.1	Snyk (developer security platform)	Code Injection	N/A	N/A	https://snyk.io/ https://www.cve.org/CVERecord?id=CVE-2024-21571
https://nvd.nist.gov/vuln/detail/CVE-2024-10516	8.1	Swift Performance Lite plugin for WordPress	Path Traversal	all versions up to, and including, 2.3.7.1	N/A	https://wordpress.org/plugins/swift-performance-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4921f41a-a9b1-4ae2-a903-c14ed22dcc15?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-11178	8.1	Login With OTP plugin for WordPress	Authentication Bypass	up to, and including, 1.4.2	N/A	https://wordpress.org/plugins/otp-login/ https://www.wordfence.com/threat-intel/vulnerabilities/id/d3775d48-5985-475e-8fb9-c4c5fd044772?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-47115	7.8	IBM AIX	OS Command Injection	7.2, 7.3 and VIOS 3.1 and 4.1	N/A	https://www.ibm.com/products/aix https://www.ibm.com/support/pages/node/7178033
https://nvd.nist.gov/vuln/detail/CVE-2024-49600	7.8	Dell Power Manager	Improper Access Control	prior to 3.17	N/A	https://www.dell.com/support/contents/el-gr/article/product-support/self-support-knowledgebase/software-and-downloads/dell-power-manager https://www.dell.com/support/kbdoc/en-us/000244438/dsa-2024-439
https://nvd.nist.gov/vuln/detail/CVE-2024-54216	7.7	ARForms	Path Traversal	from n/a through 6.4.1	N/A	https://www.arformsplugin.com/ https://patchstack.com/database/wordpress/plugin/arforms/vulnerability/wordpress-arforms-plugin-6-4-1-subscriber-arbitrary-file-read-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-53817	7.6	Acowebs Product Labels For Woocommerce	SQL Injection	from n/a through 1.5.8	N/A	https://acowebs.com/woocommerce-product-labels/ https://patchstack.com/database/wordpress/plugin/aco-product-labels-for-woocommerce/vulnerability/wordpress-acowebs-product-labels-for-woocommerce-plugin-1-5-8-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-53919	7.6	Barco ClickShare CX-30/20, C-5/10, and ClickShare Bar Pro	OS-level command execution as root	before 2.21.1	N/A	https://www.barco.com/en https://www.barco.com/en/support/knowledge-base/15008-clickshare-cve-2024-53919

https://nvd.nist.gov/vuln/detail/CVE-2024-11585	7.5	WP Hide & Security Enhancer plugin for WordPress	Path Traversal	all versions up to, and including, 2.5.1	N/A	https://wordpress.org/plugins/wp-hide-security-enhancer/ https://www.wordfence.com/threat-intel/vulnerabilities/id/43c7056e-39d8-467e-92ec-33a31e5dafc9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-54151	7.5	Directus real-time API	Exposure of Sensitive Information to an Unauthorized Actor	version 11.0.0 and prior to version 11.3.0	N/A	https://directus.io/toolkit/realtime https://github.com/directus/directus/security/advisories/GHSA-849r-qrwj-8rv4
https://nvd.nist.gov/vuln/detail/CVE-2024-11010	7.2	FileOrganizer – Manage WordPress and Website Files plugin for WordPress	Path Traversal	all versions up to, and including, 1.1.4	N/A	https://wordpress.org/plugins/fileorganizer/ https://www.wordfence.com/threat-intel/vulnerabilities/id/8e958653-36c4-4979-89e1-d9411a35a92a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10247	7.2	Video Gallery – Best WordPress YouTube Gallery Plugin plugin for WordPress	SQL Injection	all versions up to, and including, 2.4.2	N/A	https://el.wordpress.org/plugins/gallery-videos/ https://www.wordfence.com/threat-intel/vulnerabilities/id/f5524582-5aac-48b4-ad67-7c4829d63ed0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-54197	7.2	SAP NetWeaver Administrator	Server-Side Request Forgery (SSRF)	N/A	N/A	https://help.sap.com/doc/saphelp_scm700_ehp02/7.0.2/en-US/49/49b19720cc3b5be10000000a42189b/content.htm https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
Vulnerability Summary for the Week of December 2, 2024	Review Full list	https://www.cisa.gov/news-events/bulletins/sb24-344
CISA listed Over 270 Critical Vulnerabilities That Were Fixed Last Week – What's New!	ABB ASPECT-Enterprise Suite WordPress Plugins IoT and Networking Devices ROS2 (Robotic Operating System) Django Google Chrome Android Devices	https://cybersecuritynews.com/cisa-vulnerability-bulletin/

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
Compromised Software Code Poses New Systemic Risk to U.S. Critical Infrastructure	https://www.darkreading.com/application-security/compromised-software-code-poses-systemic-risks-to-critical-infrastructure
8Base ransomware group **hacked Croatia's Port** of Rijeka	https://securityaffairs.com/171779/cyber-crime/8base-ransomware-croatias-port-of-rijeka.html
Romania Cancels Presidential Election Results After Alleged Russian Meddling on TikTok	https://thehackernews.com/2024/12/romania-cancels-presidential-election.html
WAF Vulnerability in Akamai, Cloudflare, and Imperva Affected 40% of Fortune 100 Companies	https://cybersecuritynews.com/waf-vulnerability-in-akamai-cloudflare-and-imperva/
THN Recap: Top Cybersecurity Threats, Tools and Tips (Dec 2 - 8)	https://thehackernews.com/2024/12/thn-recap-top-cybersecurity-threats_9.html
Outdated Google Workspace Sync blocks **Windows 11 24H2 upgrades**	https://www.bleepingcomputer.com/news/microsoft/outdated-google-workspace-sync-blocks-windows-11-24h2-upgrades/
Let's Encrypt to End Support for Online Certificate Status Protocol (OCSP)	https://cybersecuritynews.com/lets-encrypt-ocsp-end-support/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Anna Jacques Hospital **Ransomware** Breach Hits 316K Patients	https://www.infosecurity-magazine.com/news/anna-jacques-hospital-ransomware/
New Atrium **Health data breach** impacts 585,000 individuals	https://securityaffairs.com/171747/data-breach/atrium-health-disclosed-a-data-breach.html
Black Basta Ransomware **Breaches BT Conferencing**	https://dailysecurityreview.com/security-spotlight/black-basta-ransomware-breaches-bt-conferencing/
Cipla Allegedly Hacked, Akira Ransomware Claims **70GB Data Stolen**	https://cybersecuritynews.com/cipla-allegedly-hacked/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
New **Windows zero-day** exposes NTLM credentials, gets unofficial patch	https://www.bleepingcomputer.com/news/security/new-windows-zero-day-exposes-ntlm-credentials-gets-unofficial-patch/
Critical **Windows Zero-Day** Alert: No Patch Available Yet for Users	https://hackread.com/windows-zero-day-alert-no-patch-available-for-users/
OpenWrt Supply Chain Attack Via SHA-256 Collision & Command Injection	https://cybersecuritynews.com/openwrt-supply-chain-attack/
Synology Router Vulnerabilities Let Attackers Inject Arbitrary Web Script	https://cybersecuritynews.com/synology-router-vulnerabilities/
MC LR Router and GoCast unpatched vulnerabilities	https://blog.talosintelligence.com/mc-lr-router-and-gocast-zero-day-vulnerabilities-2/
Mauri Ransomware Exploiting **Apache ActiveMQ** Vulnerability	https://cybersecuritynews.com/mauri-ransomware-exploiting-apache-activemq/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Phishing **Scam Targets Ukrainian Defense Companies**	https://www.infosecurity-magazine.com/news/phishing-scam-targets-ukrainian/
Intrusions targeting **I-O Data router zero-days** underway	https://www.scworld.com/brief/intrusions-targeting-i-o-data-router-zero-days-underway
RedLine info-stealer campaign targets Russian businesses through pirated corporate software	https://securityaffairs.com/171771/cyber-crime/redline-info-stealer-campaign-targets-russian-businesses.html

Romania 's election systems hit by 85,000 attacks ahead of presidential vote	https://securityaffairs.com/171758/cyber-warfare-2/romanias-election-systems-hit-by-85000-attacks.html
Additional **Pegasus spyware**-hit devices identified	https://www.scworld.com/brief/additional-pegasus-spyware-hit-devices-identified
Romanian energy supplier **Electrica Group is facing a ransomware attack**	https://securityaffairs.com/171832/hacking/electrica-group-ransomware-attack.html
Ransomware attack hits leading heart surgery device maker	https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-leading-heart-surgery-device-maker/
Russian hacktivists target oil, gas and water sectors worldwide	https://www.scworld.com/news/russian-hacktivist-groups-target-oil-and-gas-and-water-sectors-worldwide
New Meeten **Malware Targets macOS and Windows** Users to Steal Login Credentials	https://cybersecuritynews.com/meeten-ai-malware-attacking-macos-windows/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Top **cybersecurity books for your holiday gift** list	https://www.helpnetsecurity.com/2024/12/09/cybersecurity-books-gift-ideas/

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 διάφορους 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