Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 13/12/2024 - 17/12/2024

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-2024-21576	**10**	ComfyUI-Bmad-Nodes	Code Injection	N/A	N/A	https://github.com/comfyanonymous/ComfyUI https://github.com/bmad4ever/comfyui_bmad_nodes/blob/392af9490cbadf32a1fe92ff820ebabe88c51ee8/cv_nodes.py#L1814
https://nvd.nist.gov/vuln/detail/CVE-2024-55877	**9.9**	XWiki Platform	Improper Neutralization of Directives	Starting in version 9.7-rc-1 and prior to versions 15.10.11, 16.4.1, and 16.5.0	N/A	https://www.xwiki.org/xwiki/bin/view/Main/WebHome https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-2r87-74cx-2p7c
https://nvd.nist.gov/vuln/detail/CVE-2024-12356	**9.8**	Privileged Remote Access (PRA) and Remote Support (RS) (Beyond Trust products)	Command Injection	N/A	N/A	https://www.beyondtrust.com/ https://www.beyondtrust.com/trust-center/security-advisories/bt24-10
https://nvd.nist.gov/vuln/detail/CVE-2024-43234	**9.8**	Envato Security Team Woffice	Authentication Bypass	from n/a through 5.4.14	N/A	https://elements.envato.com/wordpress/plugins/security https://patchstack.com/database/wordpress/theme/woffice/vulnerability/wordpress-woffice-theme-5-4-14-unauthenticated-account-takeover-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-49775	**9.8**	Opcenter Execution Foundation	Heap-based Buffer Overflow	All versions	N/A	https://plm.sw.siemens.com/en-US/opcenter/execution/foundation-oee/ https://cert-portal.siemens.com/productcert/html/ssa-928984.html
https://nvd.nist.gov/vuln/detail/CVE-2024-55956	**9.8**	Cleo Harmony	Incorrect Default Permissions	before 5.8.0.24, VLTrader before 5.8.0.24, and LexiCom before 5.8.0.24	N/A	https://www.cleo.com/cleo-harmony https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Advisory-CVE-Pending https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update
https://nvd.nist.gov/vuln/detail/CVE-2024-11986	**9.6**	CrushFTP	Cross-site Scripting	N/A	N/A	https://crushftp.com/index.html https://crushftp.com/crush11wiki/Wiki.jsp?page=Update
https://nvd.nist.gov/vuln/detail/CVE-2024-10205	**9.4**	Hitachi Ops Center Analyzer	Missing Authentication for Critical Function	Hitachi Ops Center Analyzer: from 10.0.0-00 before 11.0.3-00; Hitachi Infrastructure Analytics Advisor: from 2.1.0-00 through 4.4.0-00	N/A	https://docs.hitachivantara.com/r/en-us/ops-center-analyzer/10.9.x/mk-99ana002 https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2024-151/index.html

https://nvd.nist.gov/vuln/detail/CVE-2024-54234	9.3	wp-buy Limit Login Attempts	SQL Injection	from n/a through 5.5	N/A	https://wordpress.org/plugins/wp-limit-login-attempts/ https://patchstack.com/database/wordpress/plugin/wp-limit-failed-login-attempts/vulnerability/wordpress-limit-login-attempts-plugin-5-5-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-54285	9.1	SeedProd LLC SeedProd Pro	Unrestricted Upload of File with Dangerous Type	from n/a through 6.18.10	N/A	https://www.seedprod.com/ https://patchstack.com/database/wordpress/plugin/seedprod-coming-soon-pro-5/vulnerability/wordpress-seedprod-pro-plugin-6-18-10-remote-code-execution-rce-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-55969	9.1	DocIO in Syncfusion Essential Studio	XMLExceptio n	before 27.1.55	N/A	https://help.syncfusion.com/document-processing/word/word-library/net/create-word-document-in-asp-net-core https://ej2.syncfusion.com/aspnetmvc/documentation/release-notes/27.1.55?type=all
https://nvd.nist.gov/vuln/detail/CVE-2023-29476	9.1	Menlo On-Premise Appliance	Inconsistent Interpretatio n of HTTP Requests	N/A	2.88.2+, 2.89.1+, and 2.90.1+	https://info.menlosecurity.com/rs/281-OWV-899/images/Menlo-Migrating-On-Premise-Proxy-to-SWG-SB.pdf https://www.menlosecurity.com/published-security-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-11834	9.1	PlexTrac	Path Traversal	from 1.61.3 before 2.8.1	N/A	https://plextrac.com/ https://docs.plextrac.com/plextrac-documentation/master/security-advisories#release-2.11.0
https://nvd.nist.gov/vuln/detail/CVE-2024-55661	8.8	Laravel Pulse	Code Injection	prior to version 1.3.1	N/A	https://pulse.laravel.com/ https://github.com/laravel/pulse/security/advisories/GHSA-8vwh-pr89-4mw2
https://nvd.nist.gov/vuln/detail/CVE-2023-33996	8.8	CleanTalk - Anti-Spam Protection	Missing Authorization	from n/a through 6.10	N/A	https://cleantalk.org/ https://patchstack.com/database/wordpress/plugin/cleantalk-spam-protect/vulnerability/wordpress-spam-protection-antispam-firewall-by-cleantalk-plugin-6-10-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-12092	8.7	ENOVIA Collaborative Industry Innovator	Cross-site Scripting	Release 3DEXPERIENCE R2024x	N/A	https://www.3ds.com/support/news/3dexperience-r2024x-fd03-program-directory-now-available https://www.3ds.com/vulnerability/advisories
https://nvd.nist.gov/vuln/detail/CVE-2024-52063	8.6	RTI Connext Professional	Classic Buffer Overflow	from 7.0.0 before 7.3.0.5, from 6.1.0 before 6.1.2.21, from 6.0.0 before 6.0.1.40, from 5.0.0 before 5.3.1.45	N/A	https://www.rti.com/products/connext-professional https://www.rti.com/vulnerabilities/#cve-2024-52063
https://nvd.nist.gov/vuln/detail/CVE-2023-38385	8.3	Artbees JupiterX Core	Missing Authorization	from 3.0.0 through 3.3.0	N/A	https://jupiterx.artbees.net/home/ https://patchstack.com/database/wordpress/plugin/jupiterx-core/vulnerability/wordpress-jupiter-x-core-plugin-3-0-0-3-3-0-multiple-contributor-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-56083	8.1	Cognition Devin	Out-of-bounds Read	before 2024-12-12	N/A	https://www.cognition.ai/ https://trust.cognition.ai/
https://nvd.nist.gov/vuln/detail/CVE-2024-11721	8.1	Frontend Admin by DynamiApps plugin for WordPress	Improper Privilege Management	all versions up to, and including, 3.24.5	N/A	https://wordpress.com/plugins/acf-frontend-form-element https://www.wordfence.com/threat-intel/vulnerabilities/id/e9fdc833-8384-42c0-ad9b-72e5b6351964?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2024-10783	8.1	MainWP Child – Securely Connects to the MainWP Dashboard to Manage Multiple Sites plugin for WordPress	Missing Authorization	all versions up to, and including, 5.2	N/A	https://wordpress.org/plugins/mainwp/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9156e536-a58e-4d78-b136-af8a9613ee23?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-54139	7.9	Combodo iTop	Cross-site Scripting	Prior to versions 2.7.11, 3.1.2, and 3.2.0	2.7.11, 3.1.2, and 3.2.0	https://www.combodo.com/itop-193 https://github.com/Combodo/iTop/security/advisories/GHSA-jmv2-wfh5-h5wg
https://nvd.nist.gov/vuln/detail/CVE-2024-31891	7.8	IBM Storage Scale GUI	Execution with Unnecessary Privileges	5.1.9.0 through 5.1.9.6 and 5.2.0.0 through 5.2.1.1	N/A	https://www.ibm.com/docs/en/storage-scale/5.1.9?topic=overview-introduction-storage-scale-gui https://www.ibm.com/support/pages/node/7178098
https://nvd.nist.gov/vuln/detail/CVE-2024-8058	7.6	FileZ client	Improper Validation of Specified Type of Input	N/A	N/A	https://www.filez.com/ https://www.filez.com/securityPolicy/1.html?1733849740
https://nvd.nist.gov/vuln/detail/CVE-2024-56073	7.5	FastNetMon Community Edition	Divide By Zero	through 1.2.7	N/A	https://fastnetmon.com/ https://cwe.mitre.org/data/definitions/369.html https://github.com/pavel-odintsov/fastnetmon/commit/a36718525e08ad0f2a809363001bf105efc5fe1c
https://nvd.nist.gov/vuln/detail/CVE-2024-10095	7.4	Progress Telerik UI for WPF	Deserialization of Untrusted Data	prior to 2024 Q4 (2024.4.1213)	N/A	https://www.telerik.com/products/wpf/overview.aspx https://docs.telerik.com/devtools/wpf/knowledge-base/kb-security-unsafe-deserialization-vulnerability-cve-2024-10095
https://nvd.nist.gov/vuln/detail/CVE-2024-10646	7.2	Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder plugin for WordPress	Cross-site Scripting	all versions up to, and including, 5.2.6	N/A	https://wordpress.org/plugins/fluentform/ https://www.wordfence.com/threat-intel/vulnerabilities/id/41c2ec31-360d-4145-b0b4-77d4d1d4b8a1?source=cve

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-2024-20767 Adobe ColdFusion Improper Access Control Vulnerability CVE-2024-35250 Microsoft Windows Kernel-Mode Driver Untrusted Pointer Dereference Vulnerability CVE-2024-50623 Cleo Multiple Products Unrestricted File Upload Vulnerability	https://www.cisa.gov/news-events/alerts/2024/12/16/cisa-adds-two-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2024/12/13/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Requests Public Comment for Draft National Cyber Incident Response Plan Update	Cybersecurity Best Practices, Critical Infrastructure Security and Resilience, Partnerships and Collaboration	https://www.cisa.gov/news-events/alerts/2024/12/16/cisa-requests-public-comment-draft-national-cyber-incident-response-plan-update
CISA Releases Industrial Control Systems Advisories	ICSA-24-352-01 ThreatQuotient ThreatQ Platform ICSA-24-352-02 Hitachi Energy TropOS Devices Series 1400/2400/6400 ICSA-24-352-03 Rockwell Automation PowerMonitor 1000 Remote ICSA-24-352-04 Schneider Electric Modicon ICSMA-24-352-01 BD Diagnostic Solutions Products	https://www.cisa.gov/news-events/alerts/2024/12/17/cisa-releases-five-industrial-control-systems-advisories
CISA Warns of Adobe & Windows Kernel Driver Exploited in Attacks	CVE-2024-20767: Adobe ColdFusion Improper Access Control Vulnerability CVE-2024-35250: Microsoft Windows Kernel-Mode Driver Untrusted Pointer Dereference Vulnerability	https://cybersecuritynews.com/cisa-warns-of-adobe-windows-kernel-driver/

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
With DORA approaching, financial institutions must strengthen their cyber resilience	https://www.helpnetsecurity.com/2024/12/16/financial-institutions-dora-requirements/
Resecurity introduces Government Security Operations Center (GSOC) at NATO Edge 2024	https://hackread.com/resecurity-government-security-operations-center-gsoc-nato-edge-2024/
Germany Disrupts BADBOX Malware on 30,000 Devices Using Sinkhole Action	https://thehackernews.com/2024/12/germany-disrupts-badbox-malware-on.html
Russia blocks Viber in latest attempt to censor communications	https://www.bleepingcomputer.com/news/security/russia-blocks-viber-in-latest-attempt-to-censor-communications/
Salt Typhoon	https://billatnapier.medium.com/salt-typhoon-10d0ac7d9228

Microsoft Blocks 7000 Password Attacks/sec – 1 Billion Password to be Replaced With "Passkey"	https://cybersecuritynews.com/microsoft-to-delete-1-billion-password-to-replace-passkey/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Clop ransomware claims responsibility for Cleo data theft attacks	https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-cleo-data-theft-attacks/
Canadian Eyecare Firm Care1 Exposes 2.2TB of Patient Records	https://hackread.com/canadian-eyecare-firm-care1-exposes-patient-records/
Serbian Authorities Use Novispy Spyware & Cellebrite Forensic Tools to Hack Journalists	https://cybersecuritynews.com/authorities-use-novispy-spyware/
Rhode Island confirms data breach after Brain Cipher ransomware attack	https://www.bleepingcomputer.com/news/security/rhode-island-confirms-data-breach-after-brain-cipher-ransomware-attack/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
390,000 WordPress accounts stolen from hackers in supply chain attack	https://www.bleepingcomputer.com/news/security/390-000-wordpress-accounts-stolen-from-hackers-in-supply-chain-attack/
U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Cleo Harmony, VLTrader, and LexiCom flaw to its Known Exploited Vulnerabilities catalog.	https://securityaffairs.com/171973/security/u-s-cisa-adds-cleo-harmony-vltrader-and-lexicom-flaw-to-its-known-exploited-vulnerabilities-catalog.html
Tic TAC Alert: A Remote Code Execution Vulnerability in Medical Imaging	https://cybersecuritynews.com/tic-tac-alert/
Curl Vulnerability Let Attackers Access Sensitive Information	https://cybersecuritynews.com/curl-vulnerability-attackers-sensitive-information/
Windows kernel bug now exploited in attacks to gain SYSTEM privileges	https://www.bleepingcomputer.com/news/security/windows-kernel-bug-now-exploited-in-attacks-to-gain-system-privileges/
Multiple flaws in Volkswagen Group's infotainment unit allow for vehicle compromise	https://securityaffairs.com/172024/hacking/volkswagen-group-infotainment-unit-flaws.html
RCE Vulnerability in 1,000,000 WordPress Sites Lets Attackers Gain Control Over Backend	https://cybersecuritynews.com/wordpress-sites-vulnerable-to-critical-rce/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
PUMAKIT, a sophisticated rootkit that uses advanced stealth mechanisms	https://securityaffairs.com/172016/malware/pumakit-sophisticated-rootkit.html
IOCONTROL cyberweapon used to target infrastructure in the US and Isreael	https://securityaffairs.com/171980/malware/iocontrol-cyberweapon-targets-us-isreael.html
Russian cyberspies target Android users with new spyware	https://www.bleepingcomputer.com/news/security/russian-cyberspies-target-android-users-with-new-spyware/
Iranian malware linked to recent attacks on US, Israeli infrastructure	https://www.scworld.com/news/iranian-malware-linked-to-recent-attacks-on-us-israeli-infrastructure
CISA warns water facilities to secure HMI systems exposed online	https://www.bleepingcomputer.com/news/security/cisa-warns-water-facilities-to-secure-hmi-systems-exposed-online/
Hackers Scanning RDP Services Especially Port 1098 For Exploitation	https://cybersecuritynews.com/hackers-scanning-rdp-services/
Malicious ads push Lumma infostealer via fake CAPTCHA pages	https://www.bleepingcomputer.com/news/security/malicious-ads-push-lumma-infostealer-via-fake-captcha-pages/
Microsoft Teams Vishing Spreads DarkGate RAT	https://www.darkreading.com/cyberattacks-data-breaches/vishing-via-microsoft-teams-spreads-darkgate-rat
MUT-1244 targeting security researchers, red teamers, and threat actors	https://www.helpnetsecurity.com/2024/12/16/mut-1244-targeting-security-researchers-threat-aws-wordpress-data-theft/
Hackers Leverage Red Team Tools in RDP Attacks Via TOR & VPN for Data Exfiltration	https://cybersecuritynews.com/hackers-leverage-red-team-tools-in-rdp-attacks/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Guarding Linux Systems from Account Takeovers: Proven Security Tactics	https://infosecwriteups.com/guarding-linux-systems-from-account-takeovers-proven-security-tactics-13903ee7f70e
Citrix shares mitigations for ongoing Netscaler password spray attacks	https://www.bleepingcomputer.com/news/security/citrix-shares-mitigations-for-ongoing-netscaler-password-spray-attacks/
Top 15 Firewall Management Tools in 2025	https://cybersecuritynews.com/firewall-management-tools/
10 Best Web Scanners for Website Security In 2025	https://cybersecuritynews.com/web-scanners/
THN Weekly Recap: Top Cybersecurity Threats, Tools and Tips	https://thehackernews.com/2024/12/thn-recap-top-cybersecurity-threats_16.html

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/