Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 10/12/2024 - 13/12/2024

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-2024-11639	**10**	Ivanti CSA	Authentication Bypass	before 5.0.3	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-2024-11639-CVE-2024-11772-CVE-2024-11773
https://nvd.nist.gov/vuln/detail/CVE-2024-42448	**9.9**	VSPC management agent	Remote Code Execution	N/A	N/A	https://helpcenter.veeam.com/docs/vac/provider_admin/manage_vac_agents.html?ver=81 https://www.veeam.com/kb4679
https://nvd.nist.gov/vuln/detail/CVE-2024-55877	**9.9**	XWiki Platform	Improper Neutralization of Directives	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/ https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-2r87-74cx-2p7c
https://nvd.nist.gov/vuln/detail/CVE-2024-23538	**9.9**	Apache Fineract	Improper Neutralization of Special Elements	<1.8.5	N/A	https://fineract.apache.org/ https://cwiki.apache.org/confluence/display/FINERACT/Apache+Fineract+Security+Report
https://nvd.nist.gov/vuln/detail/CVE-2024-11015	**9.8**	Sign In With Google plugin for WordPress	Improper Authentication	all versions up to, and including, 1.8.0	N/A	https://wordpress.org/plugins/login-with-google/ https://www.wordfence.com/threat-intel/vulnerabilities/id/afe894b0-5e91-4aa2-bbd1-1f74274701cf?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-11948	**9.8**	GFI Archiver Telerik Web UI	Remote Code Execution	N/A	N/A	https://gfi.ai/ https://www.zerodayinitiative.com/advisories/ZDI-24-1671/
https://nvd.nist.gov/vuln/detail/CVE-2024-46442	**9.8**	BYD Dilink Headunit System	Improper Restriction of Excessive Authentication Attempts	v3.0 to v4.0	N/A	https://www.byd.com/en-ma/support/dilink http://byd.com https://github.com/zgsnj123/BYD_headunit_vuls/tree/main
https://nvd.nist.gov/vuln/detail/CVE-2024-12286	**9.8**	MOBATIME Network Master Clock	Use of Default Credentials	DTS 4801	N/A	https://www.mobatime.com/product-category/master-clock/ https://www.cisa.gov/news-events/ics-advisories/icsa-24-345-01
https://nvd.nist.gov/vuln/detail/CVE-2024-45494	**9.8**	MSA Safety FieldServer Gateways	Incorrect Default Permissions	before 7.0.0	N/A	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-2024-54751	**9.8**	COMFAST CF-WR630AX	Incorrect Default Permissions	v2.7.0.2	N/A	https://sihaijialan.en.made-in-china.com/product/MtFrLKojrucH/China-Comfast-CF-Wr630ax-WiFi6-3000Mbps-Wireless-Mesh-WiFi-Router.html

						https://colorful-meadow-5b9.notion.site/CF-WR630AX_HardCode_vuln-14bc216a1c3080968161ce15e35fa652?pvs=4
https://nvd.nist.gov/vuln/detail/CVE-2024-55586	9.8	Nette Database	Improper Neutralization of Special Elements	through 3.2.4	N/A	https://doc.nette.org/en/database https://www.csirt.sk/nette-framework-vulnerability-permits-sql-injection.html
https://nvd.nist.gov/vuln/detail/CVE-2024-5660	9.8	ARM products	Exposure of Resource to Wrong Sphere	A77, A78, A78C, A78AE, A710, V1, V2, V3, V3AE, X1, X1C, X2, X3, X4, N2, X925 & Travis	N/A	https://www.arm.com/ https://developer.arm.com/Arm%20Security%20Center/Arm%20CPU%20Vulnerability%20CVE-2024-5660
https://nvd.nist.gov/vuln/detail/CVE-2024-53552	9.8	CrushFTP	Weak Password Recovery Mechanism for Forgotten Password	10 before 10.8.3 and 11 before 11.2.3	N/A	https://www.crushftp.com/index.html https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update
https://nvd.nist.gov/vuln/detail/CVE-2024-49147	9.3	Microsoft Update Catalog	Deserialization of Untrusted Data	N/A	N/A	https://www.catalog.update.microsoft.com/Home.aspx https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49147
https://nvd.nist.gov/vuln/detail/CVE-2024-11053	9.1	curl	curl could leak the password	N/A	N/A	https://curl.se/ http://www.openwall.com/lists/oss-security/2024/12/11/1 https://curl.se/docs/CVE-2024-11053.html
https://nvd.nist.gov/vuln/detail/CVE-2024-55884	9	Mullvad VPN client	heap-based out-of-bounds writes	2024.6 (Desktop), 2024.8 (iOS), and 2024.8-beta1 (Android)	N/A	https://mullvad.net/en/download/vpn/windows https://x41-dsec.de/news/2024/12/11/mullvad/
https://nvd.nist.gov/vuln/detail/CVE-2024-10590	8.8	Opt-In Downloads plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 4.07	N/A	https://wordpress.org/plugins/optin-forms/ https://www.wordfence.com/threat-intel/vulnerabilities/id/5c3c20b8-12cf-4ce6-a1d4-99204df33fcd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-46340	8.8	TP-Link TL-WR845N	Cleartext Storage of Sensitive Information	V4_200909 and V4_190219	N/A	https://www.tp-link.com/in/home-networking/wifi-router/tl-wr845n/ https://security.iiita.ac.in/iot/factory-reset.docx
https://nvd.nist.gov/vuln/detail/CVE-2024-50930	8.8	Silicon Labs Z-Wave Series 500	Improper Preservation of Permissions	v6.84.0	N/A	https://www.silabs.com/wireless/z-wave/500-series-modules https://github.com/CNK2100/2024-CVE/blob/main/README.md
https://nvd.nist.gov/vuln/detail/CVE-2024-50920	8.8	Silicon Labs (SiLabs) Z-Wave Series 700 and 800	Improper Preservation	v7.21.1	N/A	https://www.silabs.com/wireless/z-wave/introduction-to-z-wave-800-series https://github.com/CNK2100/2024-CVE/blob/main/README.md

			of Permissions			
https://nvd.nist.gov/vuln/detail/CVE-2024-53247	8.8	Splunk Enterprise	Deserialization of Untrusted Data	below 9.3.2, 9.2.4, and 9.1.7, and versions below 3.2.461 and 3.7.13 of the Splunk Secure Gateway	N/A	https://www.splunk.com/en_us/products/enterprise-security.html https://advisory.splunk.com/advisories/SVD-2024-1205
https://nvd.nist.gov/vuln/detail/CVE-2024-42407	8.5	Gallagher Command Centre Alarm Transmitter	Insertion of Sensitive Information into Log File	Multiple versions	N/A	https://security.gallagher.com/en/Product-Ranges/Command-Centre https://security.gallagher.com/en-NZ/Security-Advisories/CVE-2024-42407
https://nvd.nist.gov/vuln/detail/CVE-2024-11205	8.5	WPForms plugin for WordPress	Missing Authorization	starting from 1.8.4 up to, and including, 1.9.2.1	N/A	https://wordpress.org/plugins/wpforms-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/66898509-a93c-4dc3-bf01-1743daaa0ff1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-53290	8.4	Dell ThinOS	Command Injection	version 2408	N/A	https://www.dell.com/en-us/lp/dell-thinos https://www.dell.com/support/kbdoc/en-us/000248475/dsa-2024-463
https://nvd.nist.gov/vuln/detail/CVE-2024-47484	8.2	Dell Avamar	SQL Injection	19.9	N/A	https://www.dell.com/en-us/lp/dt/data-protection-suite-avamar-protection-software https://www.dell.com/support/kbdoc/en-us/000258636/dsa-2024-489-security-update-for-dell-avamar-and-dell-avamar-virtual-edition-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-10111	8.1	OAuth Single Sign On – SSO (OAuth Client) plugin for WordPress	Improper Authentication	all versions up to, and including, 6.26.3	N/A	https://wordpress.org/plugins/miniorange-login-with-eve-online-google-facebook/ https://www.wordfence.com/threat-intel/vulnerabilities/id/ddd83877-739f-4c21-8179-20de8bbc4936?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-45404	8.1	OpenCTI	Improper Authentication	below 6.2.18	N/A	https://filigran.io/solutions/open-cti/ https://github.com/OpenCTI-Platform/opencti/security/advisories/GHSA-hg56-r6hh-56j7
https://nvd.nist.gov/vuln/detail/CVE-2024-11950	7.8	XnSoft XnView Classic	Integer Underflow	N/A	N/A	https://www.xnview.com/en/ https://www.zerodayinitiative.com/advisories/ZDI-24-1640/
https://nvd.nist.gov/vuln/detail/CVE-2024-54095	7.8	Solid Edge SE2024	Integer Underflow	All versions < V224.0 Update 10	N/A	https://blogs.sw.siemens.com/solidedge/introducing-solid-edge-2024/ https://cert-portal.siemens.com/productcert/html/ssa-730188.html
https://nvd.nist.gov/vuln/detail/CVE-2024-4109	7.5	Undertow web server	Exposure of Sensitive Information to an Unauthorized Actor	N/A	N/A	https://undertow.io/ https://access.redhat.com/security/cve/CVE-2024-4109 https://bugzilla.redhat.com/show_bug.cgi?id=2272325
https://nvd.nist.gov/vuln/detail/CVE-2024-53292	7.2	Dell VxVerify	Plaintext Storage of a Password	prior to x.40.405	N/A	https://www.dell.com/support/kbdoc/en-us/000021527/vxrail-how-to-run-vxverify https://www.dell.com/support/kbdoc/en-us/000258964/dsa-2024-492-

						security-update-dell-vxverify-on-vxrail-plaintext-password-storage-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-54008	7.2	AirWave CLI (HPE)	OS Command Injection	N/A	N/A	https://www.arubanetworks.com/techdocs/AirWave/82130/Content/AWUserGuide/AppendixB/CLI.htm https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04765en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/CVE-2024-12363	7.1	TeamViewer Patch & Asset Management	Incorrect Permission Assignment	prior to version 24.12	N/A	https://www.teamviewer.com/ https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2024-1008/

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
Ivanti Releases Security Updates for Multiple Products	Ivanti Cloud Service Application Ivanti Desktop and Server Management (DSM) Ivanti Connect Secure and Policy Secure Ivanti Sentry Ivanti Patch SDK (This also affects Ivanti Endpoint Manager (EPM), Ivanti Security Controls, Ivanti Neurons Agent, Ivanti Neurons for Patch Management, and Ivanti Patch for Configuration Manager.)	https://www.cisa.gov/news-events/alerts/2024/12/10/ivanti-releases-security-updates-multiple-products
Microsoft Releases December 2024 Security Updates	Microsoft Security Update Guide for December	https://www.cisa.gov/news-events/alerts/2024/12/10/microsoft-releases-december-2024-security-updates
Adobe Releases Security Updates for Multiple Products	Adobe Product Security Updates for December	https://www.cisa.gov/news-events/alerts/2024/12/10/adobe-releases-security-updates-multiple-products
CISA Releases Industrial Control Systems Advisories	ICSA-24-345-01 MOBATIME Network Master Clock ICSA-24-345-02 Schneider Electric EcoStruxure Foxboro DCS Core Control Services ICSA-24-345-03 Schneider Electric FoxRTU Station ICSA-24-345-04 National Instruments LabVIEW ICSA-24-345-05 Horner Automation Cscape ICSA-24-345-06 Rockwell Automation Arena ICSA-24-338-01 Ruijie Reyee OS (Update A)	https://www.cisa.gov/news-events/alerts/2024/12/10/cisa-releases-seven-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerability to Catalog	CVE-2024-49138 Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability	https://www.cisa.gov/news-events/alerts/2024/12/10/cisa-adds-one-known-exploited-vulnerability-catalog
Apple Releases Security Updates for Multiple Products	iOS 18.2 and iPadOS 18.2 iPadOS 17.7.3 macOS Sequoia 15.2 macOS Sonoma 14.7.2 macOS Ventura 13.7.2 watchOS 11.2 tvOS 18.2 visionOS 2.2	https://www.cisa.gov/news-events/alerts/2024/12/12/apple-releases-security-updates-multiple-products

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
Experts discovered the first mobile malware families linked to Russia's Gamaredon	https://securityaffairs.com/171949/apt/gamaredon-used-two-new-android-spyware-tools.html
Chinese Cops Caught Using Android Spyware to Track Mobile Devices	https://www.darkreading.com/cyberattacks-data-breaches/chinese-cops-using-android-spyware-track-mobile-devices
Efforts to Secure US Telcos Beset by Salt Typhoon Might Fall Flat	https://www.darkreading.com/vulnerabilities-threats/efforts-secure-us-telcos-salt-typhoon
US Sanctions Chinese Cybersecurity Firm for Firewall Exploit, Ransomware Attacks	https://hackread.com/us-sanctions-chinese-cybersecurityfirm-firewall-ransomware/
Operation PowerOFF took down 27 DDoS platforms across 15 countries	https://securityaffairs.com/171909/cyber-crime/operation-poweroff-took-down-27-ddos-platforms.html
FBI warns of rising AI tools deployment in financial fraud schemes	https://www.scworld.com/brief/fbi-warns-of-rising-ai-tools-deployment-in-financial-fraud-schemes
Understand and Combat the Top Healthcare Cloud Threats Today	https://www.infosecurity-magazine.com/webinars/understanding-healthcare-cloud/
New Malware Technique Could Exploit Windows UI Framework to Evade EDR Tools	https://thehackernews.com/2024/12/new-malware-technique-could-exploit.html
Containers have 600+ vulnerabilities on average	https://www.helpnetsecurity.com/2024/12/11/containers-security-concerns/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
IoT Cloud Cracked by 'Open Sesame' Over-the-Air Attack	https://www.darkreading.com/ics-ot-security/iot-cloud-cracked-open-sesame-attack
Data Breach Exposes 765,000 Senior Dating Website Users	https://dailysecurityreview.com/security-spotlight/data-breach-exposes-765000-senior-dating-website-users/
Chinese Hacker Pwns 81K Sophos Devices With Zero-Day Bug	https://www.darkreading.com/cyberattacks-data-breaches/chinese-hacker-pwns-81k-sophos-devices-with-zero-day-bug

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Cleo patches critical zero-day exploited in data theft attacks	https://www.bleepingcomputer.com/news/security/cleo-patches-critical-zero-day-exploited-in-data-theft-attacks/
Security Flaws in WordPress Woffice Theme Prompts Urgent Update	https://www.infosecurity-magazine.com/news/security-flaws-wordpress-woffice/
Several Splunk, Atlassian flaws addressed	https://www.scworld.com/brief/several-splunk-atlassian-flaws-addressed
WordPress Hunk Companion Plugin Flaw Exploited to Silently Install Vulnerable Plugins	https://thehackernews.com/2024/12/wordpress-hunk-companion-plugin-flaw.html

Critical ‘AuthQuake’ bug let attackers bypass Microsoft MFA	https://www.scworld.com/news/critical-authquake-bug-lets-attackers-bypass-microsoft-mfa
Ivanti fixed a maximum severity vulnerability in its CSA solution	https://securityaffairs.com/171850/breaking-news/ivanti-maximum-severity-flaw-csa-solution.html
Zoho QEngine: Arbitrary File Read	https://infosecwriteups.com/zoho-qengine-arbitrary-file-read-08df3d1e167e
Critical Dell Product Vulnerabilities Let Attackers Compromise Affected Systems	https://cybersecuritynews.com/dell-vulnerabilities-alert/
Microsoft Office & Excel Vulnerabilities Expose Systems To RCE & Privilege Escalation	https://cybersecuritynews.com/office-and-excel-vulnerabilities-allows-rce-attacks/
Windows Remote Desktop Services Vulnerability Let Attackers Execute Remote Code	https://cybersecuritynews.com/windows-remote-desktop-services-vulnerability/
Critical LDAP Client Vulnerability Let Attackers Gain Vulnerable System Access Remotely	https://cybersecuritynews.com/critical-ldap-client-vulnerability/
Vulnerabilities in Skoda & Volkswagen Cars Let Hackers Remotely Track Users	https://cybersecuritynews.com/vulnerabilities-skoda-volkswagen-cars/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
New stealthy Pumakit Linux rootkit malware spotted in the wild	https://www.bleepingcomputer.com/news/security/new-stealthy-pumakit-linux-rootkit-malware-spotted-in-the-wild/
336K Prometheus Instances Exposed to DoS, 'Repojacking'	https://www.darkreading.com/cloud-security/336k-prometheus-instances-exposed-dos-repojacking
New IOCONTROL malware used in critical infrastructure attacks	https://www.bleepingcomputer.com/news/security/new-iocontrol-malware-used-in-critical-infrastructure-attacks/
Russia’s Secret Blizzard APT targets Ukraine with Kazuar backdoor	https://securityaffairs.com/171896/apt/secret-blizzard-targets-ukraine-with-kazuar-backdoor.html
Lynx ransomware behind Electrica energy supplier cyberattack	https://www.bleepingcomputer.com/news/security/lynx-ransomware-behind-electrica-energy-supplier-cyberattack/
Citrix NetScaler Devices Under Attack, Brute-force Attacks Exploiting Zero-days	https://cybersecuritynews.com/citrix-netscaler-devices-under-attack/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
New infosec products of the week: December 13, 2024	https://www.helpnetsecurity.com/2024/12/13/new-infosec-products-of-the-week-december-13-2024/

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/