Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/11/2024 - 22/11/2024

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-2024-42450	**10**	Versa Director	Use of Hard-coded Credentials	N/A	22.1.4	https://versa-networks.com/ https://security-portal.versa-networks.com/emailbulletins/6735a300415abb89e9a8a9d3
https://nvd.nist.gov/vuln/detail/CVE-2024-52759	**9.8**	D-LINK DI-8003	buffer overflow	v16.07.26A1	N/A	https://www.dlink.com/gr/el https://github.com/faqiadegege/IoTVuln/blob/main/DI_8003_ip_position_asp_stackoverflow/detail.md https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2024-10094	**9.1**	Pega Platform	Code Injection	24.1.1	N/A	https://www.pega.com/products/platform https://support.pega.com/support-doc/pega-security-advisory-d24-vulnerability-remediation-note
https://nvd.nist.gov/vuln/detail/CVE-2024-34365	**9.1**	Apache Karaf Cave	Improper Input Validation	N/A	N/A	https://karaf.apache.org/cave_installation.html https://www.openwall.com/lists/oss-security/2024/05/09/5
https://nvd.nist.gov/vuln/detail/CVE-2024-11194	**8.8**	Classified Listing – Classified ads & Business Directory Plugin plugin for WordPress	Missing Authorization	all versions up to, and including, 3.1.15.1	N/A	https://wordpress.org/plugins/classified-listing/ https://www.wordfence.com/threat-intel/vulnerabilities/id/13d9a59f-1a1a-4936-a5ab-8a5e0c50303b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-48895	**8.8**	Rakuten Turbo 5G	OS Command Injection	V1.3.18 and earlier	N/A	https://corp.mobile.rakuten.co.jp/english/about/service/ https://jvn.jp/en/vu/JVNVU90667116/
https://nvd.nist.gov/vuln/detail/CVE-2024-11395	**8.8**	Google Chrome	Type Confusion	prior to 131.0.6778.85	N/A	https://www.google.com/chrome/ https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_19.html
https://nvd.nist.gov/vuln/detail/CVE-2024-21697	**8.8**	Sourcetree for Mac and Windows	Remote Code Execution	4.2.8 for Mac and 3.4.19 for Windows	N/A	https://www.sourcetreeapp.com/ https://jira.atlassian.com/browse/SRCTREE-8168
https://nvd.nist.gov/vuln/detail/CVE-2024-10913	**8.8**	Clone plugin for WordPress	Deserialization of	all versions up to, and including, 2.4.6	N/A	https://wordpress.org/plugins/wp-clone-by-wp-academy/ https://www.wordfence.com/threat-intel/vulnerabilities/id/16569267-ab52-4b96-86f0-d37c470a3938?source=cve

			Untrusted Data			
https://nvd.nist.gov/vuln/detail/CVE-2024-10979	8.8	PostgreSQL PL/Perl	execute arbitrary code	17.1, 16.5, 15.9, 14.14, 13.17, and 12.21	N/A	https://www.postgresql.org/ https://www.postgresql.org/support/security/CVE-2024-10979/
https://nvd.nist.gov/vuln/detail/CVE-2024-45419	8.1	Zoom Apps	Unchecked Return Value	N/A	N/A	https://zoom.us/download https://www.zoom.com/en/trust/security-bulletin/zsb-24041
https://nvd.nist.gov/vuln/detail/CVE-2024-52714	8.1	Tenda AC6	buffer overflow	v2.0 v15.03.06.50	N/A	https://www.tendacn.com/gr/product/ac6v5.html https://www.tendacn.com/gr/default.html
https://nvd.nist.gov/vuln/detail/CVE-2024-51503	8	Trend Micro Deep Security 20 Agent	OS Command Injection	N/A	N/A	https://help.deepsecurity.trendmicro.com/20_0/on-premise/release-notes-dsa.html https://success.trendmicro.com/en-US/solution/KA-0018154
https://nvd.nist.gov/vuln/detail/CVE-2024-52739	8	D-LINK DI-8400	Command Injection	v16.07.26A1	N/A	https://www.dlink.com https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2024-48992	7.8	Qualys	Uncontrolled Search Path Element	before version 3.8	N/A	https://www.qualys.com/ https://www.cve.org/CVERecord?id=CVE-2024-48992
https://nvd.nist.gov/vuln/detail/CVE-2024-52360	7.6	IBM Concert Software	SQL Injection	1.0.0, 1.0.1, 1.0.2, and 1.0.2.1	N/A	https://www.ibm.com/products/concert https://www.ibm.com/support/pages/node/7176346
https://nvd.nist.gov/vuln/detail/CVE-2024-11494	7.5	Zyxel P-6101C ADSL modem	Improper Authentication	P-6101CSA6AP_20140331	N/A	https://www.cleancss.com/user-manuals/i88/P6101C https://gist.github.com/stevenyu113228/78e0169d2ff110e9a65539eb29660d25
https://nvd.nist.gov/vuln/detail/CVE-2024-52598	7.5	2FAuth web app	Cross-site Scripting	5.4.1	N/A	https://docs.2fauth.app/ https://github.com/Bubka/2FAuth/security/advisories/GHSA-xwxc-w7v3-2p4j
https://nvd.nist.gov/vuln/detail/CVE-2024-34088	7.5	FRRouting	denial of service	through 9.1	N/A	https://frrouting.org/ https://github.com/FRRouting/frr/pull/15674
https://nvd.nist.gov/vuln/detail/CVE-2024-10899	7.3	The WooCommerce Product Table Lite plugin for WordPress	Code Injection	all versions up to, and including, 3.8.6	N/A	https://wordpress.org/plugins/wc-product-table-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/c9b010ff-8a4a-4553-bb2b-d58a254d7ee4?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10388	7.2	WordPress GDPR plugin for WordPress	Cross-site Scripting	all versions up to, and including, 2.0.2	N/A	https://www.welaunch.io/en/product/wordpress-gdpr/ https://www.wordfence.com/threat-intel/vulnerabilities/id/bf707d9b-2b96-4d1b-b798-38f7fe958eaf?source=cve
https://www.cve.org/CVERecord?id=CVE-2024-10788	7.2	Activity Log – Monitor & Record User	Stored Cross-Site Scripting	all versions up to, and including, 2.11.1	N/A	https://wordpress.org/plugins/aryo-activity-log/ https://www.wordfence.com/threat-intel/vulnerabilities/id/75324bf1-a00e-4da7-8d42-d224c39ceb79?source=cve

		Changes plugin for WordPress				
https://nvd.nist.gov/vuln/detail/CVE-2024-52421	7.1	WP Popup Window Maker	Cross-Site Request Forgery (CSRF)	from n/a through 2.0	N/A	https://wordpress.org/plugins/popup-maker/ https://patchstack.com/database/vulnerability/easy-popup-lightbox-maker/wordpress-wp-popup-window-maker-plugin-2-0-csrf-to-stored-xss-vulnerability?_s_id=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-2024-1212 Progress Kemp LoadMaster OS Command Injection Vulnerability CVE-2024-0012 Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability CVE-2024-9474 Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability CVE-2024-38812 VMware vCenter Server Heap-Based Buffer Overflow Vulnerability CVE-2024-38813 VMware vCenter Server Privilege Escalation Vulnerability CVE-2024-44308 Apple Multiple Products Code Execution Vulnerability CVE-2024-44309 Apple Multiple Products Cross-Site Scripting (XSS) Vulnerability CVE-2024-21287 Oracle Agile Product Lifecycle Management (PLM) Incorrect Authorization Vulnerability	https://www.cisa.gov/news-events/alerts/2024/11/18/cisa-adds-three-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2024/11/20/cisa-adds-two-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2024/11/21/cisa-adds-three-known-exploited-vulnerabilities-catalog
CISA Releases Industrial Control Systems Advisory	ICSA-24-324-01 Mitsubishi Electric MELSEC iQ-F Series ICSA-24-326-01 Automated Logic WebCTRL Premium Server ICSA-24-326-02 OSCAT Basic Library ICSA-24-326-03 Schneider Electric Modicon M340, MC80, and Momentum Unity M1E ICSA-24-326-04 Schneider Electric Modicon M340, MC80, and Momentum Unity M1E ICSA-24-326-05 Schneider Electric EcoStruxure IT Gateway ICSA-24-326-06 Schneider Electric PowerLogic PM5300 Series ICSA-24-326-07 mySCADA myPRO Manager	https://www.cisa.gov/news-events/alerts/2024/11/19/cisa-releases-one-industrial-control-systems-advisory https://www.cisa.gov/news-events/alerts/2024/11/21/cisa-releases-seven-industrial-control-systems-advisories
Apple Releases Security Updates for Multiple Products	iOS 18.1.1 and iPadOS 18.1.1 macOS Sequoia 15.1.1 iOS 17.7.2 and iPadOS 17.7.2 visionOS 2.1.1 Safari 18.1.1	https://www.cisa.gov/news-events/alerts/2024/11/20/apple-releases-security-updates-multiple-products
2024 CWE Top 25 Most Dangerous Software Weaknesses	Recommendations for Stakeholders	https://www.cisa.gov/news-events/alerts/2024/11/20/2024-cwe-top-25-most-dangerous-software-weaknesses

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
60% of Emails with QR Codes Classified as Spam or Malicious	https://www.infosecurity-magazine.com/news/60-emails-qr-codes-spam-malicious/
Oracle Linux 9 Update 5 brings security updates, OpenJDK 17, .NET 9.0	https://www.helpnetsecurity.com/2024/11/20/oracle-linux-9-update-5/
Russian Ransomware Gangs on the Hunt for Pen Testers	https://www.darkreading.com/vulnerabilities-threats/russian-ransomware-gangs-hunt-pen-testers
Ghost Tap: Hackers Exploiting NFCGate to Steal Funds via Mobile Payments	https://thehackernews.com/2024/11/ghost-tap-hackers-exploiting-nfcgate-to.html
Chinese hackers target Linux with new WolfsBane malware	https://www.bleepingcomputer.com/news/security/chinese-gelsemium-hackers-use-new-wolfsbane-linux-malware/
Microsoft Takes Action Against Phishing-as-a-Service Platform	https://www.darkreading.com/cybersecurity-operations/microsoft-takes-action-against-phishing-service-platform

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Cyberattack at French hospital exposes health data of 750,000 patients	https://www.bleepingcomputer.com/news/security/cyberattack-at-french-hospital-exposes-health-data-of-750-000-patients/
Fintech giant Finastra investigates data breach after SFTP hack	https://www.bleepingcomputer.com/news/security/fintech-giant-finastra-investigates-data-breach-after-sftp-hack/
Hot Topic Data Breach Exposes Personal Information of 56 Million Customers	https://dailysecurityreview.com/security-spotlight/hot-topic-data-breach-exposes-personal-information-of-56-million-customers/
Chinese Hackers Breached Deep Into US Telecom to Spy on Calls and Texts	https://gbhackers.com/us-telecom-hack/
Misconfigured Forces Penpals server leaks over 1.1M users' data	https://www.scworld.com/brief/misconfigured-forces-penpals-server-leaks-over-1-1m-users-data

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Decades-Old Security Vulnerabilities Found in Ubuntu's Needrestart Package	https://thehackernews.com/2024/11/decades-old-security-vulnerabilities.html

Κρίσιμη ευπάθεια Kubernetes επιτρέπει στους hackers να εκτελούν αυθαίρετο κώδικα	https://www.secnews.gr/630668/eupatheia-kubernetes-epitrepei-stous-hackers-na-ekteloun-authaireto-kwdika/
D-Link Warns of RCE Vulnerability in Legacy Routers	https://www.securityweek.com/d-link-warns-of-rce-vulnerability-in-legacy-routers/
2000+ Palo Alto Firewalls Hacked Exploiting New Vulnerabilities	https://cybersecuritynews.com/2000-palo-alto-firewalls-hacked/
FortiClient VPN Flaw Enables Undetected Brute-Force Attacks	https://gbhackers.com/forticlient-vpn-brute-force-attacks/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
FBI and CISA warn of continued cyberattacks on US telecoms	https://www.scworld.com/news/fbi-and-cisa-warn-of-continued-cyberattacks-on-us-telecoms
Hackers Hijack Jupyter Servers for Sport Stream Ripping	https://www.infosecurity-magazine.com/news/hijack-jupyter-servers-sport/
Ngioweb Botnet Fuels NSOCKS Residential Proxy Network Exploiting IoT Devices	https://thehackernews.com/2024/11/ngioweb-botnet-fuels-nsocks-residential.html
Helldown ransomware exploits Zyxel VPN flaw to breach networks	https://www.bleepingcomputer.com/news/security/helldown-ransomware-exploits-zyxel-vpn-flaw-to-breach-networks/
Warning: VMware vCenter and Kemp LoadMaster Flaws Under Active Exploitation	https://thehackernews.com/2024/11/cisa-alert-active-exploitation-of.html
Over 145,000 Industrial Control Systems Across 175 Countries Found Exposed Online	https://thehackernews.com/2024/11/over-145000-industrial-control-systems.html
Helldown ransomware exploits Zyxel VPN flaw to breach networks	https://www.bleepingcomputer.com/news/security/helldown-ransomware-exploits-zyxel-vpn-flaw-to-breach-networks/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Five backup lessons learned from the UnitedHealth ransomware attack	https://www.helpnetsecurity.com/2024/11/20/backup-strategies/
Google's AI-Powered OSS-Fuzz Tool Finds 26 Vulnerabilities in Open-Source Projects	https://thehackernews.com/2024/11/googles-ai-powered-oss-fuzz-tool-finds.html
New Windows 11 recovery tool to let admins remotely fix unbootable devices	https://www.bleepingcomputer.com/news/microsoft/windows-quick-machine-recovery-lets-admins-remotely-fix-unbootable-devices/
Gmail's New Shielded Email Feature Lets Users Create Aliases for Email Privacy	https://thehackernews.com/2024/11/shielded-email-googles-latest-tool-for.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.