Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 30/10/2024 - 01/11/2024

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-2024-51568	10	CyberPanel (aka Cyber Panel)	OS Command Injection	before 2.3.5	N/A	https://cyberpanel.net/ https://dreyand.rs/code/review/2024/10/27/what-are-my-options-cyberpanel-v236-pre-auth-rce
https://nvd.nist.gov/vuln/detail/CVE-2024-33699	9.9	LevelOne WBR-6012 router	Unverified Password Change	WBR-6012 firmware version R0.40e6	N/A	https://download.level1.info/manual/WBR-6012_UM_V1.0.pdf https://talosintelligence.com/vulnerability_reports/TALOS-2024-1984
https://nvd.nist.gov/vuln/detail/CVE-2024-9264	9.9	Grafana	remote code execution	N/A	N/A	https://grafana.com/ https://grafana.com/security/security-advisories/cve-2024-9264/
https://nvd.nist.gov/vuln/detail/CVE-2024-51482	9.9	ZoneMinder is a free, open source closed-circuit television software	SQL Injection	v1.37.* <= 1.37.64	1.37.64	https://zoneminder.com/ https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-qm8h-3xvf-m7j3
https://nvd.nist.gov/vuln/detail/CVE-2024-10392	9.8	AI Power: Complete AI Pack plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 1.8.89	N/A	https://wordpress.org/plugins/gpt3-ai-content-generator/ https://www.wordfence.com/threat-intel/vulnerabilities/id/cd8a45c9-ca48-4ea6-b34e-f05206f16155?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10456	9.8	Delta Electronics InfraSuite Device Master	Deserialization of Untrusted Data	prior to 1.0.12	N/A	https://www.deltaww.com/en-US/products/Management-System/data-center-infrasuite-device-master https://www.cisa.gov/news-events/ics-advisories/icsa-24-303-03
https://nvd.nist.gov/vuln/detail/CVE-2024-51298	9.8	Draytek Vigor3900	execute arbitrary commands	1.5.1.3	N/A	https://www.draytek.com/products/vigor3900/ https://github.com/fu37kola/cve/blob/main/DrayTek/Vigor3900/1.5.1.3/DrayTek_Vigor_3900_1.5.1.3.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-48573	9.8	AquilaCMS	SQL Injection	1.409.20 and prior	N/A	https://www.aquila-cms.com/ https://github.com/dos-m0nk3y/CVE/tree/main/CVE-2024-48573
https://nvd.nist.gov/vuln/detail/CVE-2024-48138	9.8	PluXml	Code Injection	v5.8.16 and lower	N/A	https://github.com/pluxml/PluXml https://github.com/pluxml/PluXml/issues/829
https://nvd.nist.gov/vuln/detail/CVE-2024-10488	9.8	Google Chrome	Use After Free	prior to 130.0.6723.92	N/A	https://www.google.com/chrome/ https://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_29.html https://issues.chromium.org/issues/374310077

https://nvd.nist.gov/vuln/detail/CVE-2024-48206	9.8	chainer	Deserialization of Untrusted Data	v7.8.1	N/A	https://chainer.org/ https://rumbling-slice-eb0.notion.site/chainer-s-chainermn-has-MPI-Deserialization-vulnerability-in-chainer-chainer-c6a004feb53a447e8fb440968d73d6fd
https://nvd.nist.gov/vuln/detail/CVE-2024-48063	9.8	PyTorch	Deserialization of Untrusted Data	<=2.4.1	N/A	https://pytorch.org/ https://rumbling-slice-eb0.notion.site/Distributed-RPC-Framework-RemoteModule-has-Deserialization-RCE-in-pytorch-pytorch-111e3cda9e8c8021a7d3cbc61ee1a20c
https://nvd.nist.gov/vuln/detail/CVE-2024-44256	9.3	macOS	app may be able to break out of its sandbox	N/A	Ventura 13.7.1, Sonoma 14.7.1	https://support.apple.com/en-us/109033 https://support.apple.com/en-us/121568 https://support.apple.com/en-us/121570
https://nvd.nist.gov/vuln/detail/CVE-2024-10525	9.1	Eclipse Mosquitto	Heap-based Buffer Overflow	from version 1.3.2 through 2.0.18	N/A	https://mosquitto.org/ https://mosquitto.org/blog/2024/10/version-2-0-19-released/
https://nvd.nist.gov/vuln/detail/CVE-2024-38821	9.1	Spring WebFlux applications	Authorization Bypass	N/A	N/A	https://docs.spring.io/spring-framework/reference/web/webflux.html https://spring.io/security/cve-2024-38821
https://nvd.nist.gov/vuln/detail/CVE-2024-40457	9.1	No-IP Dynamic Update Client (DUC)	cleartext credentials	v3.x	N/A	https://www.noip.com/download?page=win https://www.noip.com/support/knowledgebase/running-linux-duc-v3-0-startup-2 https://www.noip.com/support/knowledgebase/install-linux-3-x-dynamic-update-client-duc
https://nvd.nist.gov/vuln/detail/CVE-2024-10006	8.3	Consul and Consul Enterprise	Improper Neutralization of HTTP Headers	N/A	N/A	https://developer.hashicorp.com/consul/docs/intro https://discuss.hashicorp.com/t/hcsec-2024-23-consul-l7-intentions-vulnerable-to-headers-bypass
https://nvd.nist.gov/vuln/detail/CVE-2024-43383	8	Apache Lucene	Deserialization of Untrusted Data	from 4.8.0-beta00005 through 4.8.0-beta00016	N/A	https://lucene.apache.org/ https://lists.apache.org/thread/wlz1p76dxpt4rl9o29voxjd5zl7717nh
https://nvd.nist.gov/vuln/detail/CVE-2024-9419	7.8	HP Smart Universal Printing Driver	Out-of-bounds Write	N/A	N/A	https://support.hp.com/bg-en/drivers/hp-smart-universal-print-driver-series-for-windows/33835514 https://support.hp.com/us-en/document/ish_11505949-11505972-16
https://nvd.nist.gov/vuln/detail/CVE-2024-9632	7.8	X.org server	Heap-based Buffer Overflow	N/A	N/A	https://www.x.org/wiki/ https://access.redhat.com/security/cve/CVE-2024-9632
https://nvd.nist.gov/vuln/detail/CVE-2024-44080	7.5	Jitsi Meet	Cross-site Scripting	before 2.0.9779	N/A	https://meet.jit.si/ https://github.com/jitsi/security-advisories/blob/master/advisories/JSA-2024-0002.md

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
Fortinet Updates Guidance and Indicators of Compromise following FortiManager Vulnerability Exploitation	Fortinet Advisory FG-IR-24-423 CISA alert on the Fortinet FortiManager Missing Authentication Vulnerability, Google Threat Intelligence article Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)	https://www.cisa.gov/news-events/alerts/2024/10/30/fortinet-updates-guidance-and-indicators-compromise-following-fortimanager-vulnerability
Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments		https://www.cisa.gov/news-events/alerts/2024/10/31/foreign-threat-actor-conducting-large-scale-spear-phishing-campaign-rdp-attachments
CISA Releases Industrial Control Systems Advisories	ICSA-24-305-01 Rockwell Automation FactoryTalk ThinManager ICSA-24-030-02 Mitsubishi Electric FA Engineering Software Products (Update A) ICSA-24-135-04 Mitsubishi Electric Multiple FA Engineering Software Products (Update A) ICSA-23-157-02 Mitsubishi Electric MELSEC iQ-R Series/iQ-F Series (Update B)	https://www.cisa.gov/news-events/alerts/2024/10/31/cisa-releases-four-industrial-control-systems-advisories

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
Microsoft Delays Windows Copilot+ Recall Release Over Privacy Concerns	https://thehackernews.com/2024/11/microsoft-delays-windows-copilot-recall.html
50% of financial orgs have high-severity security flaws in their apps	https://www.helpnetsecurity.com/2024/11/01/financial-sector-applications-security-debt/
Fake product listings on real shopping sites lead to stolen payment information	https://www.scworld.com/news/fake-product-listings-on-real-shopping-sites-lead-to-stolen-payment-information
Sophos reveals 5-year battle with Chinese hackers attacking network devices	https://www.bleepingcomputer.com/news/security/sophos-reveals-5-year-battle-with-chinese-hackers-attacking-network-devices/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Interbank Confirms Data Breach Following Failed Extortion Attempt	https://dailysecurityreview.com/security-spotlight/interbank-confirms-data-breach-following-failed-extortion-attempt/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Hackers target critical zero-day vulnerability in PTZ cameras	https://www.bleepingcomputer.com/news/security/hackers-target-critical-zero-day-vulnerability-in-ptz-cameras/
LiteSpeed Cache WordPress plugin bug lets hackers get admin access	https://www.bleepingcomputer.com/news/security/litespeed-cache-wordpress-plugin-bug-lets-hackers-get-admin-access/
Misconfigured Git Configurations Targeted in Emeraldwhale Attack	https://www.infosecurity-magazine.com/news/emeraldwhale-targets-misconfigured/
NVIDIA shader out-of-bounds and eleven LevelOne router vulnerabilities	https://blog.talosintelligence.com/nvidia-shader-out-of-bounds-and-level1-2/
Hikvision Network Camera Flaw Let Attackers Intercept Dynamic DNS Credentials	https://cybersecuritynews.com/hikvision-network-camera-flaw/
Windows Themes zero-day bug exposes users to NTLM credential theft	https://www.theregister.com/2024/10/30/zeroday_windows_themes/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Microsoft Warns of Chinese Botnet Exploiting Router Flaws for Credential Theft	https://thehackernews.com/2024/11/microsoft-warns-of-chinese-botnet.html
New Phishing Kit Xiū gǒu Targets Users Across Five Countries With 2,000 Fake Sites	https://thehackernews.com/2024/11/new-phishing-kit-xiu-gou-targets-users.html
Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network	https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/
Canada targeted by Chinese hacking efforts	https://www.scworld.com/brief/canada-targeted-by-chinese-hacking-efforts
North Korean Hackers Collaborate with Play Ransomware	https://www.infosecurity-magazine.com/news/north-korean-hackers-collaborate/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Infosec products of the month: October 2024	https://www.helpnetsecurity.com/2024/11/01/infosec-products-of-the-month-october-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.