Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 01/11/2024 - 05/11/2024

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-2024-10653	10	IDExpert from CHANGING Information Technology	OS Command Injection	N/A	N/A	https://www.changingtec.com/EN/idexpert.html https://www.twcert.org.tw/en/cp-139-8175-57245-2.html https://www.twcert.org.tw/tw/cp-132-8174-a17fd-1.html
https://nvd.nist.gov/vuln/detail/CVE-2024-50530	9.9	Stars SMTP Mailer	Unrestricted Upload of File with Dangerous Type	from n/a through 1.7	N/A	https://wphive.com/plugins/stars-smtp-mailer/ https://patchstack.com/database/vulnerability/stars-smtp-mailer/wordpress-stars-smtp-mailer-plugin-1-7-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-7456	9.8	lunary-ai/lunary	SQL Injection	v1.4.2	N/A	https://lunary.ai/ https://huntr.com/bounties/bfb3015e-5642-4d94-ab49-e8b49c4e07e4
https://nvd.nist.gov/vuln/detail/CVE-2024-47939	9.8	Ricoh laser printers and MFPs	Stack-based Buffer Overflow	N/A	N/A	https://www.ricoh.com/printers/category01 https://www.ricoh.com/products/security/vulnerabilities/vul?id=ricoh-2024-000011
https://nvd.nist.gov/vuln/detail/CVE-2024-10595	9.8	ESAFENET CDG 5	SQL Injection	N/A	N/A	https://www.esafenet.com/ https://flowus.cn/share/651b6010-4701-4cec-a5a3-6e01e22636b9?code=G8A6P3
https://nvd.nist.gov/vuln/detail/CVE-2024-48359	9.8	Qualitor	Code Injection	v8.24	N/A	https://qualitor.net/ https://github.com/OpenXP-Research/CVE-2024-48359
https://nvd.nist.gov/vuln/detail/CVE-2024-39332	9.8	Webswing	Path Traversal	23.2.2	N/A	https://www.webswing.org/en https://herolab.usd.de/security-advisories/usd-2024-0008/
https://nvd.nist.gov/vuln/detail/CVE-2024-10731	9.8	Tongda Office Anywhere.	SQL Injection	up to 11.10	N/A	https://www.broadcom.com/support/security-center/attacksignatures/detail?asid=32178 https://github.com/LvZCh/td/issues/16
https://nvd.nist.gov/vuln/detail/CVE-2024-0105	8.9	NVIDIA ConnectX Firmware	Improper Handling of Insufficient Privileges	N/A	N/A	https://www.nvidia.com/en-us/networking/ethernet-adapters/ https://nvidia.custhelp.com/app/answers/detail/a_id/5562
https://nvd.nist.gov/vuln/detail/CVE-2024-10698	8.8	Tenda AC6	Stack-based Buffer Overflow	15.03.05.19	N/A	https://www.tendacn.com/gr/product/ac6v5.html https://github.com/theRaz0r/iot-mycve/blob/main/tenda_ac6_stackflow_formSetDeviceName/tenda_ac6_stackflow_formSetDeviceName.md

https://nvd.nist.gov/vuln/detail/CVE-2024-10662	8.8	Tenda AC15	Stack-based Buffer Overflow	15.03.05.19	N/A	https://tenda.co.hu/ https://github.com/theRaz0r/iot-mycve/blob/main/tenda_ac15_stackflow_formSetDeviceName/tenda_ac15_stackflow_formSetDeviceName.md
https://nvd.nist.gov/vuln/detail/CVE-2024-48200	8.4	MobaXterm (terminal for Windows with X11 server)	escalation of privileges	v24.2	N/A	https://mobaxterm.mobatek.net/ https://gist.github.com/ahmedsherif/ad56cd3a9ef86cdc05175fb591804c64
https://nvd.nist.gov/vuln/detail/CVE-2024-36485	8.3	Zohocorp ManageEngine	SQL Injection	8121 and prior	N/A	https://www.manageengine.com/about-us.html https://www.manageengine.com/products/active-directory-audit/cve-2024-36485.html
https://nvd.nist.gov/vuln/detail/CVE-2024-37470	8.2	WofficeIO Woffice Core	Missing Authorization	from n/a through 5.4.8	N/A	https://woffice.io/ https://patchstack.com/database/vulnerability/woffice-core/wordpress-woffice-core-plugin-5-4-8-unauthenticated-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-45893	8	DrayTek Vigor3900	OS Command Injection	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-2024-38421	7.8	qualcomm (multiple vulnerabilities)	Use After Free	N/A	N/A	https://www.qualcomm.com/ https://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html
https://nvd.nist.gov/vuln/detail/CVE-2024-51672	7.6	WPDeveloper BetterLinks	SQL Injection	from n/a through 2.1.7	N/A	https://wordpress.org/plugins/betterlinks/ https://patchstack.com/database/vulnerability/betterlinks/wordpress-betterlinks-plugin-2-1-7-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-9191	7.1	Okta Device Access	Incorrect Default Permissions	N/A	N/A	https://help.okta.com/oie/en-us/content/topics/oda/oda-overview.htm https://trust.okta.com/security-advisories/
https://nvd.nist.gov/vuln/detail/CVE-2024-43235	7.1	MetaBox.Io Meta Box – WordPress Custom Fields Framework	Missing Authorization	from n/a through 5.9.10	N/A	https://el.wordpress.org/plugins/meta-box/ https://patchstack.com/database/vulnerability/meta-box/wordpress-meta-box-plugin-5-9-10-broken-access-control-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-2024-8957 PTZOptics PT30X-SDI/NDI Cameras OS Command Injection Vulnerability CVE-2024-8956 PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability	https://www.cisa.gov/news-events/alerts/2024/11/04/cisa-adds-two-known-exploited-vulnerabilities-catalog

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
ChatGPT-4o can be used for autonomous voice-based scams	https://www.bleepingcomputer.com/news/security/chatgpt-4o-can-be-used-for-autonomous-voice-based-scams/
Microsoft warns Azure Virtual Desktop users of black screen issues	https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-azure-virtual-desktop-users-of-black-screen-issues/
Schneider Electric Hacked and Blackmailed Following Lumma Infostealer Infection	https://www.infostealers.com/article/schneider-electric-hacked-and-blackmailed-due-to-lumma-infostealer-infection/
Novel phishing campaign targets Windows systems with malicious Linux VMs	https://www.scworld.com/brief/novel-phishing-campaign-targets-windows-systems-with-malicious-linux-vms
Chinese Air Fryers May Be Spying on Consumers, Which? Warns	https://www.infosecurity-magazine.com/news/chinese-air-fryers-spying/

3.1 Breaches

News - Breaches

Σύντομη περιγραφή / Τίτλος	URL
About 87K compromised in Mystic Valley Elder Services breach	https://www.scworld.com/brief/about-87k-compromised-in-mystic-valley-elder-services-breach
Massive Git Config Breach Exposes 15,000 Credentials; 10,000 Private Repos Cloned	https://thehackernews.com/2024/11/massive-git-config-breach-exposes-15000.html
City of Columbus Ransomware Attack: 500,000 Individuals Affected by Rhysida Ransomware Data Breach	https://dailysecurityreview.com/security-spotlight/city-of-columbus-ransomware-attack-500000-individuals-affected-by-rhysida-ransomware-data-breach/
Nokia purportedly breached by IntelBroker	https://www.scworld.com/brief/nokia-purportedly-breached-by-intelbroker

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Week in review: Windows Themes spoofing bug "returns", employees phished via Microsoft Teams	https://www.helpnetsecurity.com/2024/11/03/week-in-review-windows-themes-spoofing-bug-returns-employees-phished-via-microsoft-teams/
Synology Urges Patch for Critical Zero-Click RCE Flaw Affecting Millions of NAS Devices	https://thehackernews.com/2024/11/synology-urges-patch-for-critical-zero.html
Google patches actively exploited Android vulnerability (CVE-2024-43093)	https://www.helpnetsecurity.com/2024/11/05/cve-2024-43093/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
New FakeCall Malware Variant Hijacks Android Devices for Fraudulent Banking Calls	https://thehackernews.com/2024/11/new-fakecall-malware-variant-hijacks.html
Meet Interlock — The new ransomware targeting FreeBSD servers	https://www.bleepingcomputer.com/news/security/meet-interlock-the-new-ransomware-targeting-freebsd-servers/
Chinese threat actors use Quad7 botnet in password-spray attacks	https://securityaffairs.com/170503/malware/quad7-botnet-used-by-chinese-threat-actors.html
LastPass warns of fake support centers trying to steal customer data	https://www.bleepingcomputer.com/news/security/lastpass-warns-of-fake-support-centers-trying-to-steal-customer-data/
Active exploitation of PTZOptics zero-days underway	https://www.scworld.com/brief/active-exploitation-of-ptzoptics-zero-days-underway
US and Israel Warn of Iranian Threat Actor's New Tradecraft	https://www.infosecurity-magazine.com/news/us-israel-iran-new-tradecraft/
Iranian APT Group Targets IP Cameras, Extends Attacks Beyond Israel	https://www.darkreading.com/vulnerabilities-threats/iranian-group-targets-ip-cameras-extends-attacks-beyond-israel
Android Botnet 'ToxicPanda' Bashes Banks Across Europe, Latin America	https://www.darkreading.com/application-security/android-botnet-toxicpanda-bashes-banks-europe-latin-america
DocuSign's API used to lure victims into e-signing fake invoices	https://www.scworld.com/news/docusigns-api-used-to-lure-victims-into-e-signing-fake-invoices

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**

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.