Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 05/11/2024 - 08/11/2024

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-2024-51567	**10**	CyberPanel	bypass authentication	Versions through 2.3.6 and (unpatched) 2.3.7	N/A	https://cyberpanel.net/ https://cyberpanel.net/blog/detials-and-fix-of-recent-security-issue-and-patch-of-cyberpanel
https://nvd.nist.gov/vuln/detail/CVE-2024-20418	**10**	Cisco Unified Industrial Wireless Software for Cisco Ultra-Reliable Wireless Backhaul (URWB) Access Points	unauthenticated, remote attacker to perform command injection	N/A	N/A	https://www.cisco.com/site/us/en/products/networking/industrial-wireless/index.html https://nvd.nist.gov/vuln/detail/CVE-2024-20418
https://nvd.nist.gov/vuln/detail/CVE-2024-47575	**9.8**	FortiManager	missing authentication	FortiManager 7.6.0, FortiManager 7.4.0 through 7.4.4, FortiManager 7.2.0 through 7.2.7, FortiManager 7.0.0 through 7.0.12, FortiManager 6.4.0 through 6.4.14, FortiManager 6.2.0 through 6.2.12, Fortinet FortiManager Cloud 7.4.1 through 7.4.4, FortiManager Cloud 7.2.1 through 7.2.7, FortiManager Cloud 7.0.1 through 7.0.12, FortiManager Cloud 6.4.1 through 6.4.7	N/A	https://fortimanager.forticloud.com/ https://fortiguard.fortinet.com/psirt/FG-IR-24-423
https://nvd.nist.gov/vuln/detail/CVE-2024-49368	**9.8**	Nginx UI	Unchecked logrotate settings lead to arbitrary command execution	< 2.0.0-beta.36	ersion 2.0.0-beta.36	https://nginxui.com/ https://github.com/0xJacky/nginx-ui/security/advisories/GHSA-66m6-27r9-77vm

https://nvd.nist.gov/vuln/detail/CVE-2024-45216	9.8	Apache Solr	Authentication bypass	from 5.3.0 before 8.11.4, from 9.0.0 before 9.7.0	9.7.0, or 8.11.4	https://solr.apache.org/ https://solr.apache.org/security.html#cve-2024-45216-apache-solr-authentication-bypass-possible-using-a-fake-url-path-ending
https://nvd.nist.gov/vuln/detail/CVE-2024-51358	9.8	Linux Server Heimdall	execute arbitrary code	v.2.6.1	N/A	https://docs.linuxserver.io/images/docker-heimdall/ https://github.com/Kov404/CVE-2024-51358
https://nvd.nist.gov/vuln/detail/CVE-2024-43491	9.8	Microsoft Windows Update	Remote Code Execution	Windows 10, version 1507 (initial version released July 2015)	N/A	https://learn.microsoft.com/en-us/windows/release-health/status-windows-10-1507 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491
https://nvd.nist.gov/vuln/detail/CVE-2024-25675	9.8	MISP	client does not need to use POST to start an export generation process	before 2.4.184	N/A	https://www.misp-project.org/ https://github.com/MISP/MISP/compare/v2.4.183...v2.4.184
https://nvd.nist.gov/vuln/detail/CVE-2024-51504	9.1	ZooKeeper Admin Server (Apache)	Authentication bypass	N/A	3.9.3	https://zookeeper.apache.org/doc/r3.5.1-alpha/zookeeperAdmin.html https://lists.apache.org/thread/b3qrmpkto5r6989qr61fw9y2x646kqlh
https://nvd.nist.gov/vuln/detail/CVE-2024-47460	9	PAPI (Aruba's Access Point management protocol)	Command injection	N/A	N/A	https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/papi-enha-secu/enha-secu.htm https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04722en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/CVE-2024-21833	8.8	Multiple TP-LINK products	execution of arbitrary OS commands by unauthenticated attacker with access to the product	N/A	N/A	https://www.tp-link.com/gr/ https://www.tp-link.com/jp/support/download/archer-ax3000/#Firmware https://www.tp-link.com/jp/support/download/archer-ax5400/#Firmware https://www.tp-link.com/jp/support/download/archer-axe75/#Firmware https://www.tp-link.com/jp/support/download/deco-x50/v1/#Firmware https://www.tp-link.com/jp/support/download/deco-xe200/#Firmware
https://nvd.nist.gov/vuln/detail/CVE-2024-51116	8.8	Tenda AC6	buffer overflow	v2.0 V15.03.06.50	N/A	https://www.tendacn.com/gr/product/ac6v5.html https://github.com/CLan-nad/CVE/blob/main/tenda/formSetPPTPServer/readme.md
https://nvd.nist.gov/vuln/detail/CVE-2024-20536	8.8	Cisco Nexus Dashboard Fabric Controller (NDFC)	SQL Injection	N/A	N/A	https://www.cisco.com/c/en_uk/products/cloud-systems-management/prime-data-center-network-manager/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-sqli-CyPPAxrL
https://nvd.nist.gov/vuln/detail/CVE-2024-32305	8.8	Tenda A18	stack overflow	v15.03.05.05	N/A	https://www.tendacn.com/product/a18.html https://github.com/abcdefg-png/IoT-vulnerable/blob/main/Tenda/AC18/fromWizardHandle.md
https://nvd.nist.gov/vuln/detail/CVE-2024-38286	8.6	Apache Tomcat	Denial of Service	from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1	Users are recommended to upgrade to version	https://tomcat.apache.org/ https://lists.apache.org/thread/wms60cvbsz3fpbz9psxtfx8r41jl6d4s

				through 10.1.24, from 9.0.13 through 9.0.89. Older, unsupported versions may also be affected	11.0.0-M21, 10.1.25, or 9.0.90	
https://nvd.nist.gov/vuln/detail/CVE-2024-36485	8.3	Zohocorp ManageEngine ADAudit Plus	SQL Injection	below 8121	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-2024-21250	8.1	Oracle Process Manufacturing Product Development product of Oracle E-Business Suite	unauthorized creation, deletion or modification access to critical data	12.2.13-12.2.14	N/A	https://www.oracle.com/a/ocom/docs/opm-product-development-062105.pdf https://www.oracle.com/security-alerts/cpuoct2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-10914	8.1	D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L	os command injection	up to 20241028	N/A	https://www.dlink.com/gr/el/products/dns-320-2-bay-sharecenter-network-storage-enclosure https://netsecfish.notion.site/Command-Injection-Vulnerability-in-name-parameter-for-D-Link-NAS-12d6b683e67c80c49ffcc9214c239a07
https://nvd.nist.gov/vuln/detail/CVE-2024-10011	8.1	BuddyPress plugin for WordPress	Directory Traversal	all versions up to, and including, 14.1.0	N/A	https://wordpress.org/plugins/buddypress/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4327f414-64f4-4193-a5c0-2a5ecdd75e11?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-21885	7.8	X.Org server	heap buffer overflow	N/A	N/A	https://www.x.org/wiki/ https://access.redhat.com/security/cve/CVE-2024-21885
https://nvd.nist.gov/vuln/detail/CVE-2024-21763	7.5	BIG-IP AFM Device	BIG-IP AFM vulnerability	N/A	N/A	https://www.f5.com/products/big-ip-services/advanced-firewall-manager https://my.f5.com/manage/s/article/K000137521
https://nvd.nist.gov/vuln/detail/CVE-2024-20484	7.5	External Agent Assignment Service (EAAS) feature of Cisco Enterprise Chat and Email (ECE)	Chat and Email Denial of Service Vulnerability	N/A	N/A	https://www.cisco.com/c/en/us/support/docs/contact-center/enterprise-chat-email/215837-troubleshoot-ece-route-chat-to-agent-fai.pdf https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-dos-Oqb9uFEv
https://nvd.nist.gov/vuln/detail/CVE-2024-9139	7.2	Moxa products	OS Command Injection	N/A	N/A	https://www.moxa.com/en https://www.moxa.com/en/support/product-support/security-advisory/mpsa-241154-missing-authentication-and-os-command-injection-vulnerabilities-in-routers-and-network-security-appliances

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 CVE-2024-43093 Android Framework Privilege Escalation Vulnerability CVE-2024-51567 CyberPanel Incorrect Default Permissions Vulnerability CVE-2019-16278 Nostromo nhttpd Directory Traversal Vulnerability CVE-2024-5910 Palo Alto Expedition Missing Authentication Vulnerability	https://www.cisa.gov/news-events/alerts/2024/11/04/cisa-adds-two-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2024/11/07/cisa-adds-four-known-exploited-vulnerabilities-catalog
CISA Releases Industrial Control Systems Advisories	ICSA-24-312-01 Beckhoff Automation TwinCAT Package Manager ICSA-24-312-02 Delta Electronics DIAScreen ICSA-24-312-03 Bosch Rexroth IndraDrive	https://www.cisa.gov/news-events/alerts/2024/11/07/cisa-releases-three-industrial-control-systems-advisories

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
New CRON#TRAP Malware Infects Windows by Hiding in Linux VM to Evade Antivirus	https://thehackernews.com/2024/11/new-crontrap-malware-infects-windows-by.html
A closer look at the 2023-2030 Australian Cyber Security Strategy	https://www.helpnetsecurity.com/2024/11/08/australian-cyber-security-strategy-video/
Hackers Leverage Okta Phishing Attacks to Target FCC and Popular Crypto Firms	https://dailysecurityreview.com/security-spotlight/okta-phishing-attacks-target-fcc-and-crypto-firms/
Canada Closes TikTok Offices, Citing National Security	https://www.darkreading.com/cyber-risk/canada-closes-tiktok-offices-national-security
New SteelFox Malware Posing as Popular Software to Steal Browser Data	https://hackread.com/steelfox-malware-software-to-steal-browser-data/
Attacks with novel SteelFox trojan hit Windows machines	https://www.scworld.com/brief/attacks-with-novel-steelfox-trojan-hit-windows-machines

German Law Could Protect Researchers Reporting Vulns	https://www.darkreading.com/cybersecurity-operations/germany-law-protect-researchers-reporting-vulns
VEILDrive Attack Exploits Microsoft Services to Evade Detection and Distribute Malware	https://thehackernews.com/2024/11/veildrive-attack-exploits-microsoft.html
IBM Security Verify Access impacted by dozens of bugs	https://www.scworld.com/brief/ibm-security-verify-access-impacted-by-dozens-of-bugs
South Korea fined Meta $15.67M for illegally collecting and sharing Facebook users	https://securityaffairs.com/170618/digital-id/south-korea-fined-meta-15-67m.html

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Memorial Hospital and Manor suffered a ransomware attack	https://securityaffairs.com/170629/cyber-crime/memorial-hospital-and-manor-ransomware-attack.html

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Critical Palo Alto Networks Expedition bug exploited (CVE-2024-5910)	https://www.helpnetsecurity.com/2024/11/08/cve-2024-5910/
Cisco Bug Could Lead to Command Injection Attacks	https://www.darkreading.com/vulnerabilities-threats/cisco-bug-command-injection-attacks
HPE warns of critical RCE flaws in Aruba Networking access points	https://www.bleepingcomputer.com/news/security/hpe-warns-of-critical-rce-flaws-in-aruba-networking-access-points/
Maximum severity Cisco URWB vulnerability addressed	https://www.scworld.com/brief/maximum-severity-cisco-urwb-vulnerability-addressed
Critical vulnerability in Cisco industrial wireless access points fixed (CVE-2024-20418)	https://www.helpnetsecurity.com/2024/11/07/cve-2024-20418/
Active exploitation of Android vulnerabilities ongoing	https://www.scworld.com/brief/active-exploitation-of-android-vulnerabilities-ongoing
Synology fixed critical flaw impacting millions of DiskStation and BeePhotos NAS devices	https://securityaffairs.com/170602/hacking/synology-fixed-critical-bug-in-diskstation-and-beephotos-nas.html

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**

North Korean Actor Deploys Novel Malware Campaign Against Crypto Firms	https://www.infosecurity-magazine.com/news/north-korea-novel-malware-crypto/
Threat actors use copyright infringement phishing lure to deploy infostealers	https://www.infostealers.com/article/threat-actors-use-copyright-infringement-phishing-lure-to-deploy-infostealers/
Interlock Ransomware Targets US Healthcare, IT and Government Sectors	https://www.infosecurity-magazine.com/news/interlock-ransomware-us-healthcare/
China-Aligned MirrorFace Hackers Target EU Diplomats with World Expo 2025 Bait	https://thehackernews.com/2024/11/china-aligned-mirrorface-hackers-target.html
Updated Strela Stealer malware hits Germany, Spain	https://www.scworld.com/brief/updated-strela-stealer-malware-hits-germany-spain

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
NCSC Publishes Tips to Tackle Malvertising Threat	https://www.infosecurity-magazine.com/news/ncsc-publishes-tips-tackle/

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.