Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 22/11/2024 - 26/11/2024

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-2024-47407	10	mySCADA myPRO Manager	OS Command Injection	N/A	N/A	https://www.myscada.org/ https://www.cisa.gov/news-events/ics-advisories/icsa-24-326-07
https://nvd.nist.gov/vuln/detail/CVE-2024-45496	9.9	OpenShift Container Platform (Redhat)	misuse of elevated privileges	N/A	N/A	https://www.redhat.com/en/technologies/cloud-computing/openshift https://access.redhat.com/security/cve/CVE-2024-45496
https://nvd.nist.gov/vuln/detail/CVE-2024-53915	9.8	Veritas Enterprise Vault	remote attackers to execute arbitrary code	before 15.2, ZDI-CAN-24405	N/A	https://www.veritas.com/insights/enterprise-vault https://www.veritas.com/content/support/en_US/security/VTS24-014
https://nvd.nist.gov/vuln/detail/CVE-2024-7012	9.8	Foreman (Redhat - Apache mod_proxy)	authentication bypass	6.13, 6.14 and 6.15	N/A	https://theforeman.org/ https://access.redhat.com/security/cve/CVE-2024-7012
https://nvd.nist.gov/vuln/detail/CVE-2024-0138	9.8	NVIDIA Base Command Manager	missing authentication	N/A	N/A	https://docs.nvidia.com/base-command-manager/index.html https://nvidia.custhelp.com/app/answers/detail/a_id/5595
https://nvd.nist.gov/vuln/detail/CVE-2024-9511	9.8	FluentSMTP – WP SMTP Plugin with Amazon SES, SendGrid, MailGun, Postmark, Google and Any SMTP Provider plugin for WordPress	Unauthenticated PHP Object Injection	all versions up to, and including, 2.2.82	N/A	https://wordpress.org/plugins/fluent-smtp/ https://www.wordfence.com/threat-intel/vulnerabilities/id/a3deedc4-b939-4c54-8376-95d3728872d4?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-0012	9.8	Palo Alto Networks PAN-OS software	Authentication Bypass	PAN-OS 10.2, PAN-OS 11.0, PAN-OS 11.1, and PAN-OS 11.2	Cloud NGFW and Prisma Access are not impacted	https://docs.paloaltonetworks.com/pan-os https://security.paloaltonetworks.com/CVE-2024-0012
https://nvd.nist.gov/vuln/detail/CVE-2024-52533	9.8	GNOME Glib	buffer overflow	before 2.82.1	N/A	https://docs.gtk.org/glib/ https://gitlab.gnome.org/GNOME/glib/-/issues/3461
https://nvd.nist.gov/vuln/detail/CVE-2024-52765	9.8	H3C GR-1800AX MiniGRW1B0V100R007	remote code execution	N/A	N/A	https://www.h3c.com/en/Products_and_Solutions/SMB_Products/Router/ http://tjr181.com/2024/11/08/H3C%20GR-1800AX/
https://nvd.nist.gov/vuln/detail/CVE-2024-38812	9.8	vCenter Server	Heap-overflow	N/A	N/A	https://www.vmware.com/products/cloud-infrastructure/vcenter https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968

https://nvd.nist.gov/vuln/detail/CVE-2024-48984	9.8	MBed OS	buffer overflow	6.16.0	N/A	https://os.mbed.com/mbed-os/ https://github.com/mbed-ce/mbed-os/pull/387
https://nvd.nist.gov/vuln/detail/CVE-2024-9707	9.8	Hunk Companion plugin for WordPress	Missing Authorization	all versions up to, and including, 1.8.4	N/A	https://wordpress.org/plugins/hunk-companion/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9c101fca-037c-4bed-9dc7-baa021a8b59c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-38656	9.1	Ivanti Connect Secure and Ivanti Policy Secure	remote code execution	before version 22.7R2.2 and 9.1R18.9 before version 22.7R1.2 and 9.1R18.9	N/A	https://www.ivanti.com/products/connect-secure-vpn https://help.ivanti.com/ps/help/en_US/IPS/22.x/ag/ips_intro_pulse_policy_secure.htm https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs
https://nvd.nist.gov/vuln/detail/CVE-2024-27349	9.1	Apache HugeGraph-Server	Authentication Bypass	from 1.0.0 before 1.3.0	N/A	https://hugegraph.apache.org/ https://lists.apache.org/thread/dz9n9lndqfsf64t72o73r7sttrc6ocsd
https://www.cve.org/CVERecord?id=CVE-2024-36248	9.1	Sharp MFPs	API keys for some cloud services are hardcoded	N/A	N/A	https://global.sharp/products/copier/ https://global.sharp/products/copier/info/info_security_2024-05.html https://pierrekim.github.io/blog/2024-06-27-sharp-mfp-17-vulnerabilities.html
https://nvd.nist.gov/vuln/detail/CVE-2024-11666	9	eCharge cloud infrastructure	Unauthenticated Remote Command Injection	cph2_echarge_firmware: through 2.0.4	N/A	https://www.eocharging.com/eo-cloud https://www.onekey.com/resource/critical-vulnerabilities-in-ev-charging-stations-analysis-of-echarge-controllers
https://nvd.nist.gov/vuln/detail/CVE-2024-10979	8.8	PostgreSQL PL/Perl	execute arbitrary code	before PostgreSQL 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-2024-2698	8.8	FreeIPA - Identity, Policy, Audit	delegation rules allow a proxy service to impersonate any user to access another target service	4.11.0	N/A	https://www.freeipa.org/ https://www.freeipa.org/release-notes/4-12-1.html
https://nvd.nist.gov/vuln/detail/CVE-2024-10873	8.8	LA-Studio Element Kit for Elementor plugin for WordPress	Local File Inclusion	all versions up to, and including, 1.4.2	N/A	https://wordpress.org/plugins/lastudio-element-kit/ https://www.wordfence.com/threat-intel/vulnerabilities/id/59415c36-e48a-4c05-ad22-8d55a9e13bcd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-5924	8.8	Dropbox Desktop Folder Sharing	Mark-of-the-Web Bypass	N/A	N/A	https://www.dropbox.com/ https://www.zerodayinitiative.com/advisories/ZDI-24-677/
https://nvd.nist.gov/vuln/detail/CVE-2024-32394	8.8	Ruijie Network products	execute arbitrary code via a	RG-RSR10-01G-T(WA)-S RSR_3.0(1)B9P2_RSR10-01G-TW-	N/A	https://www.ruijienetworks.com/ https://gist.github.com/Swind1er/7aad5c28e5bdc91d73fa7489b7250c94

			crafted HTTP request	S_07150910 and RG-RSR10-01G-T(WA)-SRSR_3.0(1)B9P2_RSR10-01G-TW-S_07150910		
https://nvd.nist.gov/vuln/detail/CVE-2024-43689	8.8	ELECOM wireless access points	Stack-based buffer overflow	N/A	N/A	https://www.elecom.co.jp.e.gj.hp.transer.com/category/cat_wifi-ap/?category=client-business https://jvn.jp/en/jp/JVN24885537/
https://nvd.nist.gov/vuln/detail/CVE-2024-5725	8.8	Centreon (Monitor Anything, Anywhere)	SQL Injection Remote Code Execution	N/A	N/A	https://www.centreon.com/ https://thewatch.centreon.com/latest-security-bulletins-64/security-bulletin-for-centreon-web-3744
https://nvd.nist.gov/vuln/detail/CVE-2024-10729	8.8	Booking & Appointment Plugin for WooCommerce plugin for WordPress	Arbitrary Option Update	versions up to, and including, 6.9.0	N/A	https://www.tychesoftwares.com/docs/docs/booking-appointment-plugin-for-woocommerce-new/changelog/ https://www.wordfence.com/threat-intel/vulnerabilities/id/6ed215da-10c5-469b-bab2-923808feebd4?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-9693	8.5	GitLab CE/EE	Incorrect Authorization	all versions starting from 16.0 prior to 17.3.7, starting from 17.4 prior to 17.4.4, and starting from 17.5 prior to 17.5.2	N/A	https://about.gitlab.com/install/ce-or-ee/ https://gitlab.com/gitlab-org/gitlab/-/issues/497449
https://nvd.nist.gov/vuln/detail/CVE-2024-5608	8.3	Zohocorp ManageEngine ADAudit Plus	SQL Injection	below 8121	N/A	https://www.manageengine.com/products/active-directory-audit/ https://www.manageengine.com/products/active-directory-audit/cve-2024-5608.html
https://nvd.nist.gov/vuln/detail/CVE-2024-5154	8.1	Red Hat OpenShift Kubernetes Engine	malicious container can create symlink on host	1.30.0, 1.29.4, 1.28.6	1.30.1, 1.29.5, 1.28.7	https://www.redhat.com/en/technologies/cloud-computing/openshift/kubernetes-engine https://access.redhat.com/security/cve/CVE-2024-5154
https://nvd.nist.gov/vuln/detail/CVE-2024-10914	8.1	D-Link products	os command injection	D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028	N/A	https://www.dlink.com/gr/el https://netsecfish.notion.site/Command-Injection-Vulnerability-in-name-parameter-for-D-Link-NAS-12d6b683e67c80c49ffcc9214c239a07
https://nvd.nist.gov/vuln/detail/CVE-2024-10781	8.1	Spam protection, Anti-Spam, FireWall by CleanTalk plugin for WordPress	Authorization Bypass	all versions up to, and including, 6.44	N/A	https://wordpress.org/plugins/cleantalk-spam-protect/ https://www.wordfence.com/threat-intel/vulnerabilities/id/79ae062c-b084-4045-9407-2d94919993af?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10220	8.1	Kubernetes	arbitrary command execution	through 1.28.11, from 1.29.0 through 1.29.6, from 1.30.0 through 1.30.2	N/A	https://kubernetes.io/ https://groups.google.com/g/kubernetes-security-announce/c/ptNgV5Necko
https://nvd.nist.gov/vuln/detail/CVE-2024-52789	8	Tenda W30E	hardcoded password	v2.0 V16.01.0.8	N/A	https://www.tendacn.com/product/w30e.html https://colorful-meadow-5b9.notion.site/W30E_HardCode_vuln-13dc216a1c30805998f8d994f966760a

https://nvd.nist.gov/vuln/detail/CVE-2024-52788	8	Tenda W9	hardcoded password	v1.0.0.7(4456)	N/A	https://static.tenda.com.cn/tdeweb/download/W9/W9_Datasheet.pdf https://colorful-meadow-5b9.notion.site/W9_HardCode_vuln-13dc216a1c30800fb31bdcdca7345ec3
https://nvd.nist.gov/vuln/detail/CVE-2024-48286	8	Linksys E3000	command injection	1.0.06.002_US	N/A	https://downloads.linksys.com/downloads/userguide/Linksys_E3000_UG_USA_V10_NC-WEB.pdf https://github.com/GroundCTL2MajorTom/pocs/blob/main/Cisco_Linksys_E3000_rce.md
https://nvd.nist.gov/vuln/detail/CVE-2024-11596	7.8	Wireshark	Buffer Over-read	4.4.0 to 4.4.1 and 4.2.0 to 4.2.8	N/A	https://www.wireshark.org/ https://www.wireshark.org/security/wnpa-sec-2024-15.html
https://nvd.nist.gov/vuln/detail/CVE-2024-49597	7.6	Dell Wyse Management Suite	Improper Restriction of Excessive Authentication Attempts	versions WMS 4.4 and prior	N/A	https://www.wysemanagementsuite.com/ https://www.dell.com/support/kbdoc/en-us/000244453/dsa-2024-440
https://nvd.nist.gov/vuln/detail/CVE-2024-3657	7.5	LDAP	potential denial of service	N/A	N/A	https://ldap.com/ https://access.redhat.com/security/cve/CVE-2024-3657
https://nvd.nist.gov/vuln/detail/CVE-2024-21287	7.5	Oracle Agile PLM Framework	unauthorized access to critical data	9.3.6	N/A	https://www.oracle.com/scm/product-lifecycle-management/ https://www.oracle.com/security-alerts/alert-cve-2024-21287.html
https://nvd.nist.gov/vuln/detail/CVE-2024-52940	7.5	AnyDesk	when Allow Direct Connections is enabled	through 8.1.0 on Windows	N/A	https://anydesk.com/en https://github.com/ebrasha/abdal-anydesk-remote-ip-detector
https://nvd.nist.gov/vuln/detail/CVE-2024-10570	7.5	Security & Malware scan by CleanTalk plugin for WordPress	unauthorized SQL Injection	all versions up to, and including, 2.145	N/A	https://wordpress.org/plugins/security-malware-firewall/ https://www.wordfence.com/threat-intel/vulnerabilities/id/2187311d-6651-4eca-806d-aa2ff9fae4e2?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-49353	7.5	BM Watson Speech Services	denial of service	4.0.0 through 5.0.2	N/A	https://www.ibm.com/products/speech-to-text https://www.ibm.com/support/pages/node/7177065
https://nvd.nist.gov/vuln/detail/CVE-2024-37125	7.5	Dell SmartFabric OS10	Uncontrolled Resource Consumption	10.5.6.x, 10.5.5.x, 10.5.4.x,10.5.3.x	N/A	https://www.dell.com/en-us/shop/ipovw/open-platform-software https://www.dell.com/support/kbdoc/en-us/000228976/dsa-2024-274-security-update-for-dell-networking-os10-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-52802	7.5	RIOT (operating system for IoT)	missing check	2024.04 and prior	N/A	https://www.riot-os.org/ https://github.com/RIOT-OS/RIOT/security/advisories/GHSA-xgv3-pcq6-qmrg
https://nvd.nist.gov/vuln/detail/CVE-2024-11618	7.3	IPC Unigy Management System	server-side request forgery	04.03.00.08.0027	N/A	https://www.ipc.com/trading-communication-systems/unigy/ https://github.com/br484/br484.github.io/blob/main/archives/WEB/CVE%20-%20IPC%20Unigy%20-%20ingles.md
https://nvd.nist.gov/vuln/detail/CVE-2024-11630	7.3	E-Lins products	Backend hard-coded credentials	H685, H685f, H700, H720, H750, H820, H820Q, H820Q0 and H900 up to 3.2	N/A	https://e-lins.com/EN/ https://github.com/l3eg1nner/iot-vuln/blob/main/E-lins/Hard-Coded%20Credential%20Vulnerability%20in%20E-Lins%20Routers.md

https://nvd.nist.gov/vuln/detail/CVE-2024-28025	7.2	MC Technologies (MC LR Router 2.10.5)	OS command injection	MC LR Router 2.10.5	N/A	https://mc-technologies.com/produkt/100800/?srsltid=AfmBOop1ufHfsPiruppuCP94wq5PSeelc2336xYvfz75OYISLX5KcHpe https://talosintelligence.com/vulnerability_reports/TALOS-2024-1953
https://nvd.nist.gov/vuln/detail/CVE-2024-2419	7.1	Keycloak	path traversal	N/A	N/A	https://www.keycloak.org/ https://access.redhat.com/security/cve/CVE-2024-2419
https://nvd.nist.gov/vuln/detail/CVE-2024-9875	7.1	Okta Privileged Access server agent (SFTD)	privilege escalation	1.82.0 to 1.84.0	1.87.1 or greater	https://help.okta.com/oie/en-us/content/topics/privileged-access/server-agent/pam-configure-server-agent.htm https://help.okta.com/asa/en-us/content/topics/releasenotes/advanced-server-access-release-notes.htm

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
CISA Adds Known Exploited Vulnerability to Catalog	CVE-2023-28461 Array Networks AG and vxAG ArrayOS Improper Authentication Vulnerability	https://www.cisa.gov/news-events/alerts/2024/11/25/cisa-adds-one-known-exploited-vulnerability-catalog

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
IoT Device Traffic Up 18% as Malware Attacks Surge 400%	https://www.infosecurity-magazine.com/news/iot-device-traffic-malware-attacks/
Microsoft 365 outage impacts Exchange Online, Teams, Sharepoint	https://www.bleepingcomputer.com/news/microsoft/microsoft-365-outage-impacts-exchange-online-teams-sharepoint/
99% of UAE's .ae Domains Exposed to Phishing and Spoofing	https://hackread.com/uae-ae-domains-exposed-phishing-spoofing/
THN Recap: Top Cybersecurity Threats, Tools, and Practices (Nov 18 - Nov 24)	https://thehackernews.com/2024/11/thn-recap-top-cybersecurity-threats_25.html
North Korean Hackers Steal $10M with AI-Driven Scams and Malware on LinkedIn	https://thehackernews.com/2024/11/north-korean-hackers-steal-10m-with-ai.html
Massive Credit Card Leak, Database of 1,221,551 Cards Circulating on Dark Web	https://gbhackers.com/massive-credit-card-leak/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Faraway Russian hackers breached US organization via Wi-Fi	https://www.helpnetsecurity.com/2024/11/25/enterprise-wi-fi-compromised/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
QNAP addresses critical flaws across NAS, router software	https://www.bleepingcomputer.com/news/security/qnap-addresses-critical-flaws-across-nas-router-software/
More than 400K devices vulnerable to most exploited flaws	https://www.scworld.com/brief/more-than-400k-devices-vulnerable-to-most-exploited-flaws
Neighboring Wi-Fi networks exploited in APT28 attack	https://www.scworld.com/brief/neighboring-wi-fi-networks-exploited-in-apt28-attack
Week in review: 0-days exploited in Palo Alto Networks firewalls, two unknown Linux backdoors identified	https://www.helpnetsecurity.com/2024/11/24/week-in-review-0-days-exploited-in-palo-alto-networks-firewalls-two-unknown-linux-backdoors-identified/
Critical Vulnerabilities Found in Anti-Spam Plugin Used by 200,000 WordPress Sites	https://www.securityweek.com/critical-vulnerabilities-found-in-anti-spam-plugin-used-by-200000-wordpress-sites/
Massive Credit Card Leak, Database of 1,221,551 Cards Circulating on Dark Web	https://gbhackers.com/massive-credit-card-leak/
Critical 7-Zip Vulnerability Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/7-zip-vulnerability-arbitrary-code/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Zyxel firewalls targeted in recent ransomware attacks	https://securityaffairs.com/171382/cyber-crime/zyxel-firewall-ransomware-attacks.html
Asia, Europe subjected to Russian cyberespionage campaign	https://www.scworld.com/brief/asia-europe-subjected-to-russian-cyberespionage-campaign
Malware Exploits Trusted Avast Anti-Rootkit Driver to Disable Security Software	https://hackread.com/malware-avast-anti-rootkit-driver-bypass-security/
China-linked APT Gelsemium uses a new Linux backdoor dubbed WolfsBane	https://securityaffairs.com/171299/apt/china-linked-apt-gelsemium-linux-backdoor.html
RomCom Exploits Zero-Day Firefox and Windows Flaws in Sophisticated Cyberattacks	https://thehackernews.com/2024/11/romcom-exploits-zero-day-firefox-and.html
Chinese Hackers Use GHOSTSPIDER Malware to Hack Telecoms Across 12+ Countries	https://thehackernews.com/2024/11/chinese-hackers-use-ghostspider-malware.html
APT-K-47 Uses Hajj-Themed Lures to Deliver Advanced Asyncshell Malware	https://thehackernews.com/2024/11/apt-k-47-uses-hajj-themed-lures-to.html

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Google's New Restore Credentials Tool Simplifies App Login After Android Migration	https://thehackernews.com/2024/11/googles-new-restore-credentials-tool.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.