Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 29/11/2024 - 03/12/2024

Contents

1 Common Vulnerabilities and Exposures (CVE)

CVEs						
URL ευπάθειας (NIST NVD)	**CVSS v3**	**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-2024-3400	**10**	Palo Alto Networks PAN-OS	OS Command Injection	N/A	N/A	https://docs.paloaltonetworks.com/pan-os https://security.paloaltonetworks.com/CVE-2024-3400 https://unit42.paloaltonetworks.com/cve-2024-3400/ https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/
https://nvd.nist.gov/vuln/detail/CVE-2024-10905	**10**	IdentityIQ	Improper Handling of File Names	multiple versions	N/A	https://www.identityiq.com/ https://www.sailpoint.com/security-advisories/
https://nvd.nist.gov/vuln/detail/CVE-2024-49803	**9.8**	IBM Security Verify Access Appliance	OS Command Injection	10.0.0 through 10.0.8	N/A	https://www.ibm.com/docs/en/sva/10.0.8?topic=overview-security-verify-access-appliance https://www.ibm.com/support/pages/node/7177447
https://nvd.nist.gov/vuln/detail/CVE-2024-52782	**9.8**	DCME-320 (router)	Remote Code Execution	N/A	N/A	https://www.pancakumala.co.id/product/dcme-320-r2/ https://ba1100n.tech/%E6%BC%8F%E6%B4%9E%E6%8A%A5%E5%91%8A/dcme-all-series-rcessix-one/
https://nvd.nist.gov/vuln/detail/CVE-2024-50357	**9.8**	FutureNet NXR	Incorrect Provision of Specified Functionality	N/A	N/A	https://securityonline.info/century-systems-routers-vulnerable-to-remote-exploitation-cve-2024-50357-cvss-9-8/?utm_content=cmp-true https://jvn.jp/en/vu/JVNVU95001899/
https://nvd.nist.gov/vuln/detail/CVE-2024-52338	**9.8**	Apache Arrow R	Deserialization of Untrusted Data	versions 4.0.0 through 16.1.0	N/A	https://arrow.apache.org/docs/r/ https://lists.apache.org/thread/0rcbvj1gdp15lvm23zm601tjpq0k25vt

https://nvd.nist.gov/vuln/detail/CVE-2024-53915	9.8	Veritas Enterprise Vault	execute arbitrary code	before 15.2	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-2024-27198	9.8	JetBrains TeamCity	authentication bypass	before 2023.11.4	N/A	https://www.jetbrains.com/teamcity/ https://www.darkreading.com/cyberattacks-data-breaches/jetbrains-teamcity-mass-exploitation-underway-rogue-accounts-thrive https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2024-34102	9.8	Adobe Commerce	Improper Restriction of XML External Entity Reference ('XXE')	versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier	N/A	https://business.adobe.com/products/magento/magento-commerce.html https://helpx.adobe.com/security/products/magento/apsb24-40.html
https://nvd.nist.gov/vuln/detail/CVE-2024-23113	9.8	Fortinet FortiOS FortiProxy FortiPAM FortiSwitchManager	execute unauthorized code or commands via specially crafted packets	versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 versions 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3 versions 7.2.0 through 7.2.3, 7.0.0 through 7.0.3	N/A	https://www.fortinet.com https://fortiguard.com/psirt/FG-IR-24-029
https://nvd.nist.gov/vuln/detail/CVE-2024-46909	9.8	WhatsUp Gold	execute arbitrary code	before 2024.0.1	N/A	https://www.whatsupgold.com/ https://docs.progress.com/bundle/whatsupgold-release-notes-24-0/page/WhatsUp-Gold-2024.0-Release-Notes.html

https://nvd.nist.gov/vuln/detail/CVE-2024-53507	9.8	Siyuan (knowledge management system)	SQL Injection	3.1.11	N/A	https://b3log.org/siyuan/en/ https://github.com/siyuan-note/siyuan/issues/13057 https://github.com/siyuan-note/siyuan/issues/13077
https://nvd.nist.gov/vuln/detail/CVE-2024-35368	9.8	FFmpeg	Double Free	n7.0	N/A	https://www.ffmpeg.org/ https://gist.github.com/1047524396/7e6e47220ae2b2d2fb4611f0d8a31ec5
https://nvd.nist.gov/vuln/detail/CVE-2024-38476	9.8	Apache HTTP Server	information disclosure, SSRF or local script execution	2.4.59 and earlier	2.4.60	https://httpd.apache.org/ https://httpd.apache.org/security/vulnerabilities_24.html
https://nvd.nist.gov/vuln/detail/CVE-2024-49806	9.4	IBM Security Verify Access Appliance	hard coded credentials	10.0.0 through 10.0.8	N/A	https://www.ibm.com/docs/en/sva/10.0.8?topic=overview-security-verify-access-appliance https://www.ibm.com/support/pages/node/7177447
https://nvd.nist.gov/vuln/detail/CVE-2024-49360	9.2	Sandboxie	Path Traversal	N/A	N/A	https://sandboxie-plus.com/ https://github.com/sandboxie-plus/Sandboxie/security/advisories/GHSA-4chj-3c28-gvmp
https://nvd.nist.gov/vuln/detail/CVE-2024-38656	9.1	Ivanti Connect Secure	Argument injection	before version 22.7R2.2 and 9.1R18.9	N/A	https://www.ivanti.com/products/connect-secure-vpn 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-2024-28987	9.1	SolarWinds Web Help Desk (WHD)	Hardcoded Credential	N/A	N/A	https://www.solarwinds.com/web-help-desk https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28987
https://nvd.nist.gov/vuln/detail/CVE-2024-54124	8.8	Click Studios Passwordstate	Incorrect Authorization	before build 9920	N/A	https://www.clickstudios.com.au/ https://www.clickstudios.com.au/security/advisories/
https://nvd.nist.gov/vuln/detail/CVE-2024-11969	8.8	NetCloud Exchange	Incorrect Default Permissions	1.110.50	N/A	https://cradlepoint.com/datasheet/ncx-service-gateway/ https://www.incibe.es/en/incibe-cert/notices/aviso/incorrect-default-permissions-cradlepoint-netcloud-exchange
https://nvd.nist.gov/vuln/detail/CVE-2024-11960	8.8	D-Link DIR-605L	Improper Restriction	2.13B01	N/A	https://www.dlink.com/gr/el/products/dir-605l-wireless-n-300-home-cloud-router

			of Operations			https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10393
https://nvd.nist.gov/vuln/detail/CVE-2024-11699	8.8	Firefox	run arbitrary code	Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5	N/A	https://www.mozilla.org/el/firefox/new/ https://www.mozilla.org/security/advisories/mfsa2024-63/ https://www.mozilla.org/security/advisories/mfsa2024-64/ https://www.mozilla.org/security/advisories/mfsa2024-67/ https://www.mozilla.org/security/advisories/mfsa2024-68/
https://nvd.nist.gov/vuln/detail/CVE-2024-33044	8.4	Qualcomm products	Improper Validation of Array Index	N/A	N/A	https://www.qualcomm.com/ https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html
https://nvd.nist.gov/vuln/detail/CVE-2024-53979	8.2	IBM Z HMC	Cleartext Storage of Sensitive Information	N/A	1.9.3	https://www.redbooks.ibm.com/redbooks/pdfs/sg247748.pdf https://github.com/zhmcclient/zhmc-ansible-modules/security/advisories/GHSA-mw6c-f428-jx4f
https://nvd.nist.gov/vuln/detail/CVE-2024-39890	8.1	Samsung Mobile Processor	Out-of-Bounds write	Multiple products	N/A	https://semiconductor.samsung.com/processor/mobile-processor/ https://semiconductor.samsung.com/support/quality-support/product-security-updates/
https://nvd.nist.gov/vuln/detail/CVE-2024-9852	7.8	Mitsubishi Electric GENESIS64	Uncontrolled Search Path Element	all versions	N/A	https://www.mitsubishielectric.com/fa/products/software/visualisation/genesis64/index.html https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2024-010_en.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-38658	7.8	Fuji electric (V-Server)	Out-of-bounds read	v4.0.19.0 and earlier	N/A	https://monitouch.fujielectric.com/site/tellus-e/tellus03-01.html https://monitouch.fujielectric.com/site/download-e/03tellus_inf/index.php
https://nvd.nist.gov/vuln/detail/CVE-2024-12015	7.7	Project Manager' WordPress Plugin	SQL Injection	N/A	N/A	https://wordpress.org/plugins/wedevs-project-manager/ https://www.tenable.com/security/research/tra-2024-47
https://nvd.nist.gov/vuln/detail/CVE-2024-48651	7.5	ProFTPD	lack of supplemental	through 1.3.8b before cec01cc	N/A	http://www.proftpd.org/ https://github.com/proftpd/proftpd/issues/1830

			groups from mod_sql			
https://nvd.nist.gov/vuln/detail/CVE-2024-9200 https://nvd.nist.gov/vuln/detail/CVE-2024-8748	7.5	Zyxel VMG4005-B50A Zyxel VMG8825-T50K	OS Command Injection Classic Buffer Overflow	through V5.15(ABQA.2.2) C0 through V5.50(ABOM.8.4) C0	N/A	https://www.zyxel.com/global/en/products/dsl-cpe/vdsl2-17a-bonding-and-35b-single-line-bridge-vmg4005-b50a https://www.zyxel.com/global/en/products/dsl-cpe/dual-band-wireless-ac-n-vdsl2-combo-wan-gigabit-iad-vmg8825-t50khttps://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-and-post-authentication-command-injection-vulnerabilities-in-some-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-and-wifi-extenders-12-03-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-20128	7.5	Mediatek (Telephony)	Out-of-bounds Read	N/A	N/A	https://www.mediatek.com/ https://corp.mediatek.com/product-security-bulletin/December-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-45520	7.5	WithSecure Atlant (formerly F-Secure Atlant)	Out-of-bounds Read	1.0.35-1	N/A	https://www.withsecure.com/en/support/product-support/atlant https://www.withsecure.com/en/support/security-advisories/cve-2024-45520
https://nvd.nist.gov/vuln/detail/CVE-2024-53623	7.5	TP-Link ARCHER-C7	Missing Authentication for Critical Function	v5	N/A	https://www.tp-link.com/gr/home-networking/wifi-router/archer-c7/ https://github.com/Crane-c/CVE_Request/blob/main/TP-Link/C7v5/TPLink_ARCHERC7v5_unauthorized_access_vulnerability_first.md
https://nvd.nist.gov/vuln/detail/CVE-2024-36612	7.5	Zulip (Organized chat for distributed teams)	Out-of-bounds Read	from 8.0 to 8.3	N/A	https://zulip.com/ https://gist.github.com/1047524396/f7ff51d24ebbb29e21dfb70a0c97302b
https://nvd.nist.gov/vuln/detail/CVE-2024-35371	7.5	Ant-Media-Server	Out-of-bounds Read	v2.8.2	N/A	https://antmedia.io/ https://gist.github.com/1047524396/4eb17867f2e375f4824274c5e7b4d384
https://nvd.nist.gov/vuln/detail/CVE-2024-11013	7.2	NEC Corporation UNIVERGE IX	Command Injection	rom Ver9.2 to Ver10.10.21, for Ver10.8 up to Ver10.8.27, for Ver10.9 up to Ver10.9.14	N/A	https://hk.nec.com/en_HK/pdf/products/DLFE-1415.pdf https://jpn.nec.com/security-info/secinfo/nv24-009_en.html

https://nvd.nist.gov/vuln/detail/CVE-2024-45068	7.1	Hitachi Ops Center Common Services	Use of Default Credentials	10.9.3-00 before 11.0.3-00	N/A	https://docs.hitachivantara.com/r/en-us/ops-center/11.0.x/mk-99ops001/overview/overview-of-hitachi-ops-center-common-services https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2024-149/index.html

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
THN Recap: Top Cybersecurity Threats, Tools and Tips (Nov 25 - Dec 1)	https://thehackernews.com/2024/12/thn-recap-top-cybersecurity-threats.html
Bologna FC Hit By 200GB Data Theft and Ransom Demand	https://www.infosecurity-magazine.com/news/bologna-fc-200gb-data-theft/
SmokeLoader Malware Resurfaces, Targeting Manufacturing and IT in Taiwan	https://thehackernews.com/2024/12/smokeloader-malware-resurfaces.html
8 Million Android Users Hit by SpyLoan Malware in Loan Apps on Google Play	https://thehackernews.com/2024/12/8-million-android-users-hit-by-spyloan.html
Hackers stole millions of dollars from Uganda Central Bank	https://securityaffairs.com/171562/security/financially-motivated-threat-actors-hacked-ugandas-central-bank.html
Bulgarians plead guilty to spying for Russia using ‘advanced technology’	https://therecord.media/bulgarians-plead-guilty-uk-spying-russia
Poland probes Pegasus spyware abuse under the PiS government	https://securityaffairs.com/171611/intelligence/poland-probes-pegasus-spyware-abuse-under-the-pis-government.html

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
New Windows Server 2012 zero-day gets free, unofficial patches	https://www.bleepingcomputer.com/news/security/new-windows-server-2012-zero-day-gets-free-unofficial-patches/
Design flaw in Fortinet VPN server lets attackers hide logins	https://www.scworld.com/brief/design-flaw-in-fortinet-vpn-server-lets-attackers-hide-logins-1
High severity RCE flaws among several newly addressed IBM bugs	https://www.scworld.com/brief/high-severity-rce-flaws-among-several-newly-addressed-ibm-bugs-1
Microsoft re-releases Exchange updates after fixing mail delivery	https://www.bleepingcomputer.com/news/security/microsoft-re-releases-exchange-updates-after-fixing-mail-delivery/
Critical Vulnerability Found in Zabbix Network Monitoring Tool	https://www.securityweek.com/critical-vulnerability-found-in-zabbix-network-monitoring-tool/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Novel phising campaign uses corrupted Word documents to evade security	https://www.bleepingcomputer.com/news/security/novel-phising-campaign-uses-corrupted-word-documents-to-evade-security/
New Rockstar 2FA phishing service targets Microsoft 365 accounts	https://www.bleepingcomputer.com/news/security/new-rockstar-2fa-phishing-service-targets-microsoft-365-accounts/
NachoVPN Tool Exploits Flaws in Popular VPN Clients for System Compromise	https://thehackernews.com/2024/12/nachovpn-tool-exploits-flaws-in-popular.html
US government, energy sector contractor hit by ransomware	https://www.helpnetsecurity.com/2024/12/03/englobal-ransomware-attack/
Horns&Hooves Campaign Delivers RATs via Fake Emails and JavaScript Payloads	https://thehackernews.com/2024/12/horns-campaign-delivers-rats-via-fake.html
France Accuses Azerbaijan of Online Manipulation Campaigns	https://www.infosecurity-magazine.com/news/france-azerbaijan-online/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Google Chrome’s AI feature lets you quickly check website trustworthiness	https://www.bleepingcomputer.com/news/google/google-chromes-ai-feature-lets-you-quickly-check-website-trustworthiness/
OSINT Guide for Tracking Malware and Ransomware Activity	https://infosecwriteups.com/osint-guide-for-tracking-malware-and-ransomware-activity-6aaaf5e48408
Nextcloud Talk: Open-source, GDPR-compliant alternative to Microsoft Teams	https://www.helpnetsecurity.com/2024/12/03/nextcloud-talk-open-source-microsoft-teams-alternative/

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.