Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 17/12/2024 - 20/12/2024

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-2023-4617	10	Govee Home application on Android	Incorrect Authorization	Android and iOS in versions before 5.9	N/A	https://play.google.com/store/apps/details?id=com.govee.home https://cert.pl/en/posts/2024/12/CVE-2023-4617/
https://nvd.nist.gov/vuln/detail/CVE-2024-56057	9.9	VibeThemes WPLMS	Unrestricted Upload of File with Dangerous Type	from n/a before 1.9.9.5.2	N/A	https://wplms.io/ https://patchstack.com/database/wordpress/plugin/wplms-plugin/vulnerability/wordpress-wplms-plugin-1-9-9-5-2-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-21546	9.8	unisharp/laravel-filemanager	Code Injection	before 2.9.1	N/A	https://github.com/UniSharp/laravel-filemanager https://security.snyk.io/vuln/SNYK-PHP-UNISHARPLARAVELFILEMANAGER-7210316
https://nvd.nist.gov/vuln/detail/CVE-2024-50379	9.8	Apache Tomcat	Time-of-check Time-of-use (TOCTOU) Race Condition	from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0.M1 through 9.0.97	11.0.2, 10.1.34 or 9.0.08	https://tomcat.apache.org/ http://www.openwall.com/lists/oss-security/2024/12/17/4 https://lists.apache.org/thread/y6lj6q1xnp822g6ro70tn19sgtjmr80r
https://nvd.nist.gov/vuln/detail/CVE-2024-12571	9.8	Store Locator for WordPress	PHP Remote File Inclusion	3.98.9	N/A	https://wordpress.org/plugins/wp-store-locator/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4ea89a6e-e089-4e8d-afd8-2a217f6910a6?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2022-32203	9.8	HUAWEI products	Command Injection	N/A	N/A	https://www.huawei.com https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220601-01-6b47c6b6-en
https://nvd.nist.gov/vuln/detail/CVE-2024-12728	9.8	Sophos Firewall	Use of Weak Credentials	older than version 20.0 MR3 (20.0.3)	N/A	https://www.sophos.com/en-us/products/next-gen-firewall https://www.sophos.com/en-us/security-advisories/sophos-sa-20241219-sfos-rce
https://nvd.nist.gov/vuln/detail/CVE-2024-10244	9.8	ISDO Software Web Software	SQL Injection	before 3.6	N/A	https://www.isdoyazilim.com/our-services/web-software/ https://www.usom.gov.tr/bildirim/tr-24-1893
https://nvd.nist.gov/vuln/detail/CVE-2021-26102	9.8	FortiWAN	Authentication Bypass	version 4.5.7 and below, 4.4 all versions	N/A	https://docs.fortinet.com/product/fortiwan/hardware https://fortiguard.fortinet.com/psirt/FG-IR-21-048
https://nvd.nist.gov/vuln/detail/CVE-2023-34990	9.8	Fortinet FortiWLM	Relative Path Traversal	8.6.0 through 8.6.5 and 8.5.0 through 8.5.4	N/A	https://docs.fortinet.com/document/fortimanager/6.4.0/administration-guide/679601/wireless-manager-fortiwlm https://fortiguard.com/psirt/FG-IR-23-144

https://nvd.nist.gov/vuln/detail/CVE-2024-4995	9.8	Wapro ERP Desktop	Missing Encryption of Sensitive Data	before 9.00.0	N/A	https://wapro.pl/ https://cert.pl/en/posts/2024/12/CVE-2024-4995/ https://cert.pl/posts/2024/12/CVE-2024-4995/
https://nvd.nist.gov/vuln/detail/CVE-2024-12626	9.6	AutomatorWP – Automator plugin for no-code automations, webhooks & custom integrations in WordPress plugin for WordPress	Cross-site Scripting	all versions up to, and including, 5.0.9	N/A	https://el.wordpress.org/plugins/automatorwp/ https://www.wordfence.com/threat-intel/vulnerabilities/id/c8abcc7b-6c68-4fc8-81af-e88624e417dd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-37310	9.1	EVerest (EV charging software)	integer overflow	N/A	2024.3.1 and 2024.6.0	https://everest.github.io/nightly/ https://github.com/EVerest/everest-core/security/advisories/GHSA-8g9q-7qr9-vc96
https://nvd.nist.gov/vuln/detail/CVE-2024-39703	8.8	ThreatQuotient ThreatQ	Command Injection	before 5.29.3	N/A	https://www.threatq.com/ https://threatq.freshdesk.com/helpdesk/tickets/10367 https://www.cisa.gov/news-events/ics-advisories/icsa-24-352-01 https://www.threatq.com/vulnerability-management/
https://nvd.nist.gov/vuln/detail/CVE-2024-8326	8.8	s2Member – Excellent for All Kinds of Memberships, Content Restriction Paywalls & Member Access Subscriptions plugin for WordPress	Exposure of Sensitive Information to an Unauthorized Actor	all versions up to, and including, 241114	N/A	https://wordpress.org/plugins/s2member/ https://www.wordfence.com/threat-intel/vulnerabilities/id/410d4ab0-22dd-4993-afbf-ae6193b70977?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-38499	8.8	CA Client Automation (ITCM)	Improper Privilege Management	N/A	N/A	https://www.broadcom.com/info/clarity-sm/ca-client-automation https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25284
https://nvd.nist.gov/vuln/detail/CVE-2024-47093	8.8	Nagvis	Cross-site Scripting	before version 1.9.42	N/A	http://www.nagvis.org/ https://www.nagvis.org/downloads/changelog/1.9.42
https://nvd.nist.gov/vuln/detail/CVE-2020-15934	8.8	FortiClient	Improper Privilege Management	Linux versions 6.2.7 and below, version 6.4.0	N/A	https://www.fortinet.com/support/product-downloads https://www.fortiguard.com/psirt/FG-IR-20-110
https://nvd.nist.gov/vuln/detail/CVE-2024-12832	8.3	Arista NG Firewall ReportEntry	SQL Injection	N/A	N/A	https://www.arista.com/en/ug-etm-ngf/etm-ngf-getting-started https://www.zerodayinitiative.com/advisories/ZDI-24-1719/
https://nvd.nist.gov/vuln/detail/CVE-2021-32589	8.1	FortiManager	Use After Free	multiple versions	N/A	https://fortimanager.forticloud.com/ https://fortiguard.fortinet.com/psirt/FG-IR-21-067
https://nvd.nist.gov/vuln/detail/CVE-2024-56174	8.1	Optimizely Configured Commerce	Cross-site Scripting	before 5.2.2408	N/A	https://www.optimizely.com/products/configured-commerce/ https://support.optimizely.com/hc/en-us/articles/32344323720973-Configured-Commerce-Security-Advisory-COM-2024-01
https://nvd.nist.gov/vuln/detail/CVE-2024-10476	8	BD Diagnostic Solutions products	Use of Default Credentials	N/A	N/A	https://www.bd.com/en-us/products-and-solutions/solutions/diagnostic-solutions

						https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-cybersecurity-vulnerability-bulletin-diagnostic-solutions-products
https://nvd.nist.gov/vuln/detail/CVE-2024-12111	8	OpenText Privileged Access Manager	Command Injection	23.3(4.4); 24.3(4.5)	N/A	https://www.opentext.com/products/privileged-access-manager https://www.netiq.com/documentation/privileged-access-manager-45/npam_45_releasenotes/data/npam_45_releasenotes.html https://www.netiq.com/documentation/privileged-account-manager-44/npam_44_releasenotes/data/npam_44_releasenotes.html
https://nvd.nist.gov/vuln/detail/CVE-2024-47480	7.8	Dell Inventory Collector Client,	UNIX Symbolic Link (Symlink) Following	prior to 12.7.0	N/A	https://www.dell.com/support/home/en-us/drivers/driversdetails?driverid=r8px5 https://www.dell.com/support/kbdoc/en-us/000255700/dsa-2024-475
https://nvd.nist.gov/vuln/detail/CVE-2024-4230	7.8	Edgecross Basic Software for Windows	External Control of File Name or Path	versions 1.00 and later	N/A	https://www.edgecross.org/ext/en/index.html https://www.edgecross.org/client_info/EDGECROSS/view/userweb/ext/en/data-download/pdf/ECD-TE10-0003-01-EN.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-35141	7.8	IBM Security Verify Access Docker	Execution with Unnecessary Privileges	10.0.0 through 10.0.6	N/A	https://www.ibm.com/docs/en/sva/10.0.7?topic=support-docker-image-security-verify-access https://www.ibm.com/support/pages/node/7155356
https://nvd.nist.gov/vuln/detail/CVE-2022-27595	7.8	QVPN Device Client	Uncontrolled Search Path Element	QVPN Windows 2.0.0.1316 and later QVPN Windows 2.0.0.1310 and later	N/A	https://www.qnap.com/en/software/qvpn-service https://www.qnap.com/en/security-advisory/qsa-23-04
https://nvd.nist.gov/vuln/detail/CVE-2022-44520	7.8	Acrobat Reader DC	Use After Free	22.001.20085 (and earlier), 20.005.3031x (and earlier) and 17.012.30205 (and earlier)	N/A	https://get.adobe.com/reader/ https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
https://nvd.nist.gov/vuln/detail/CVE-2024-12741	7.8	NI DAQExpress	Deserialization of Untrusted Data	DAQExpress 5.1 and prior	DAQExpress is an EOL product and will not receive any updates	https://www.ni.com/en/support/downloads/software-products/download.daqexpress.html https://knowledge.ni.com/KnowledgeArticleDetails?id=kA00Z000000kFD7SAM&l=en-US
https://nvd.nist.gov/vuln/detail/CVE-2024-9624	7.6	WP All Import Pro plugin for WordPress	Server-Side Request Forgery (SSRF)	all versions up to, and including, 4.9.3	N/A	https://www.wpallimport.com/ https://www.wordfence.com/threat-intel/vulnerabilities/id/eabde2e7-5cd4-4c3e-959a-69e04f6350d3?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-47397	7.5	FXC products	Weak Authentication	AE1021 firmware versions 2.0.10 and earlier and AE1021PE firmware versions 2.0.10 and earlier	N/A	https://www.fxc.jp/en/products/wireless/AE1021.html https://jvn.jp/en/vu/JVNVU91084137/

https://nvd.nist.gov/vuln/detail/CVE-2024-4464	7.5	Synology Media Server	Authorization Bypass	before 1.4-2680, 2.0.5-3152 and 2.2.0-3325	N/A	https://www.synology.com/en-global/dsm/packages/MediaServer https://www.synology.com/en-global/security/advisory/Synology_SA_24_28
https://nvd.nist.gov/vuln/detail/CVE-2024-12025	7.5	Collapsing Categories plugin for WordPress	SQL Injection	all versions up to, and including, 3.0.8	N/A	https://wordpress.com/plugins/collapsing-categories https://www.wordfence.com/threat-intel/vulnerabilities/id/05153b11-2f26-425e-99ab-93216861802b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-9779	7.5	Open Cluster Management	Trust Boundary Violation	N/A	N/A	https://open-cluster-management.io/ https://access.redhat.com/security/cve/CVE-2024-9779
https://nvd.nist.gov/vuln/detail/CVE-2024-36832	7.5	D-Link DAP-1513	NULL Pointer Dereference	DAP-1513 REVA_FIRMWARE_1.01	N/A	https://legacy.us.dlink.com/pages/article.aspx?id=a58579daa2c1446c9bd6741ef50dc7d9 https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10396 https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2024-51479	7.5	Next.js	Improper Authorization	N/A	N/A	https://nextjs.org/ https://github.com/vercel/next.js/security/advisories/GHSA-7gfc-8cq8-jh5f
https://nvd.nist.gov/vuln/detail/CVE-2024-38819	7.5	Spring Framework	Path Traversal	N/A	N/A	https://spring.io/projects/spring-framework https://spring.io/security/cve-2024-38819
https://nvd.nist.gov/vuln/detail/CVE-2024-53270	7.5	Envoy proxy	Always-Incorrect Control Flow Implementation	N/A	1.32.3, 1.31.5, 1.30.9, and 1.29.12	https://www.envoyproxy.io/ https://github.com/envoyproxy/envoy/security/advisories/GHSA-q9qv-8j52-77p3
https://nvd.nist.gov/vuln/detail/CVE-2024-11614	7.4	DPDK's Vhost	Out-of-bounds Read	N/A	N/A	https://doc.dpdk.org/guides/sample_app_ug/vhost.html https://access.redhat.com/security/cve/CVE-2024-11614
https://nvd.nist.gov/vuln/detail/CVE-2024-12782	7.3	Fujifilm Apeos C3070	Incorrect Privilege Assignment	Apeos C3070, Apeos C5570 and Apeos C6580 up to 24.8.28	N/A	https://www.fujifilm.com/fbca/en/products/ca-multifunction-printers/apeos-c7070-c6570-c5570-c4570-c3570-c3070 https://vuldb.com/?submit.458897
https://nvd.nist.gov/vuln/detail/CVE-2024-11740	7.3	Download Manager plugin for WordPress	Code Injection	all versions up to, and including, 3.3.03	N/A	https://wordpress.org/plugins/download-manager/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4a7be578-5883-4cd3-963d-bf81c3af2003?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2023-23354	7.3	QNAP operating system	Cross-site Scripting	QuLog Center 1.5.0.738 (2023/03/06) and later QuLog Center 1.4.1.691 (2023/03/01) and later QuLog Center 1.3.1.645 (2023/02/22) and later	N/A	https://www.qnap.com/qts/4.4.1/en-us https://www.qnap.com/en/security-advisory/qsa-23-13
https://nvd.nist.gov/vuln/detail/CVE-2024-48889	7.2	FortiManager	OS Command Injection	FortiManager version 7.6.0, version 7.4.4 and below, version	N/A	https://fortimanager.forticloud.com/ https://fortiguard.fortinet.com/psirt/FG-IR-24-425

				7.2.7 and below, version 7.0.12 and below, version 6.4.14 and below and FortiManager Cloud version 7.4.4 and below, version 7.2.7 to 7.2.1, version 7.0.12 to 7.0.1		
https://nvd.nist.gov/vuln/detail/CVE-2024-51532	7.1	Dell PowerStore	Argument Injection	N/A	N/A	https://www.dell.com/en-us/shop/storage-servers-and-networking-for-business/sf/power-store https://www.dell.com/support/kbdoc/en-ie/000250483/dsa-2024-462-dell-powerstore-t-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-41165	7.1	Microsoft Word	Improper Verification of Cryptographic Signature	16.83 for macOS	N/A	https://learn.microsoft.com/en-us/officeupdates/update-history-office-for-mac https://talosintelligence.com/vulnerability_reports/TALOS-2024-1977
https://nvd.nist.gov/vuln/detail/CVE-2024-41159	7.1	Microsoft OneNote	Improper Verification of Cryptographic Signature	16.83 for macOS	N/A	https://learn.microsoft.com/en-us/officeupdates/update-history-office-for-mac https://talosintelligence.com/vulnerability_reports/TALOS-2024-1975
https://nvd.nist.gov/vuln/detail/CVE-2024-39804	7.1	Microsoft PowerPoint	Improper Verification of Cryptographic Signature	16.83 for macOS	N/A	https://learn.microsoft.com/en-us/officeupdates/update-history-office-for-mac https://talosintelligence.com/vulnerability_reports/TALOS-2024-1974

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
CISA Releases Industrial Control Systems Advisories	ICSA-24-354-01 Hitachi Energy RTU500 series CMU ICSA-24-354-02 Hitachi Energy SDM600 ICSA-24-354-03 Delta Electronics DTM Soft ICSA-24-354-04 Siemens User Management Component ICSA-24-354-05 Tibbo AggreGate Network Manager ICSA-24-354-06 Schneider Electric Accutech Manager ICSA-24-354-07 Schneider Electric Modicon Controllers	https://www.cisa.gov/news-events/alerts/2024/12/19/cisa-releases-eight-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerability to Catalog	CVE-2024-12356 BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability CVE-2018-14933 NUUO NVRmini Devices OS Command Injection Vulnerability CVE-2022-23227 NUUO NVRmini 2 Devices Missing Authentication Vulnerability CVE-2019-11001 Reolink Multiple IP Cameras OS Command Injection Vulnerability CVE-2021-40407 Reolink RLC-410W IP Camera OS Command Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2024/12/19/cisa-adds-one-known-exploited-vulnerability-catalog https://www.cisa.gov/news-events/alerts/2024/12/18/cisa-adds-four-known-exploited-vulnerabilities-catalog
CISA Releases Best Practice Guidance for Mobile Communications	Mobile Communications Best Practice Guidance.	https://www.cisa.gov/news-events/alerts/2024/12/18/cisa-releases-best-practice-guidance-mobile-communications

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
CISA: Use Signal or other secure communications app	https://www.helpnetsecurity.com/2024/12/20/cisa-guide-secure-communications-mfa-iphone-android-signal/
CISA Urges Encrypted Messaging After Salt Typhoon Hack	https://www.infosecurity-magazine.com/news/cisa-e2e-messaging-salt-typhoon/
Massive live sports piracy ring with 812 million yearly visits taken offline	https://www.bleepingcomputer.com/news/security/massive-live-sports-piracy-ring-with-812-million-yearly-visits-taken-offline/
46% of financial institutions had a data breach in the past 24 months	https://www.helpnetsecurity.com/2024/12/20/financial-industry-data-breaches/
Meta Fined $263.5m Over Data Breach in Europe	https://dailysecurityreview.com/security-spotlight/meta-fined-263-5m-over-data-breach-in-europe/
European companies hit with effective DocuSign-themed phishing emails	https://www.helpnetsecurity.com/2024/12/18/european-companies-docusign-themed-phishing-owa-microsoft-azure/
EU Sanctions Russian Cyber Actors for “Destabilizing Actions”	https://www.infosecurity-magazine.com/news/eu-sanctions-russian-cyber-actors/
European Commission Opens TikTok Election Integrity Probe	https://www.infosecurity-magazine.com/news/european-commission-tiktok-probe/

2024 roundup: Top data breach stories and industry trends	https://securityintelligence.com/articles/2024-roundup-top-data-breach-stories-and-industry-trends/
US considers banning TP-Link routers over cybersecurity risks	https://www.bleepingcomputer.com/news/security/us-considers-banning-tp-link-routers-over-cybersecurity-risks/
Windows 11 24H2 upgrades blocked on some PCs due to audio issues	https://www.bleepingcomputer.com/news/microsoft/windows-11-24h2-upgrades-blocked-on-some-pcs-due-to-audio-issues/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Ascension: Health data of 5.6 million stolen in ransomware attack	https://www.bleepingcomputer.com/news/security/ascension-health-data-of-56-million-stolen-in-ransomware-attack/
Cisco Data Leak: 2.9 Gigabytes of Source Code and Internal Documents Exposed	https://dailysecurityreview.com/security-spotlight/cisco-data-leak-2-9-gigabytes-of-source-code-and-internal-documents-exposed/
HubPhish Abuses HubSpot Tools to Target 20,000 European Users for Credential Theft	https://thehackernews.com/2024/12/hubphish-exploits-hubspot-tools-to.html

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Webcams and DVRs Vulnerable to HiatusRAT, FBI Warns	https://www.infosecurity-magazine.com/news/webcams-vulnerable-hiatusrat-fbi/
Sophos Issues Hotfixes for Critical Firewall Flaws: Update to Prevent Exploitation	https://thehackernews.com/2024/12/sophos-fixes-3-critical-firewall-flaws.html
Hackers Exploiting Critical Fortinet EMS Vulnerability to Deploy Remote Access Tools	https://thehackernews.com/2024/12/hackers-exploiting-critical-fortinet.html
Over 25,000 SonicWall VPN Firewalls exposed to critical flaws	https://www.bleepingcomputer.com/news/security/over-25-000-sonicwall-vpn-firewalls-exposed-to-critical-flaws/
Attackers Exploit Microsoft Teams and AnyDesk to Deploy DarkGate Malware	https://thehackernews.com/2024/12/attackers-exploit-microsoft-teams-and.html
Fortinet Warns of Critical FortiWLM Flaw That Could Lead to Admin Access Exploits	https://thehackernews.com/2024/12/fortinet-warns-of-critical-fortiwlm.html
Patch Alert: Critical Apache Struts Flaw Found, Exploitation Attempts Detected	https://thehackernews.com/2024/12/patch-alert-critical-apache-struts-flaw.html
Acrobat out-of-bounds and Foxit use-after-free PDF reader vulnerabilities found	https://blog.talosintelligence.com/acrobat-out-of-bounds-and-foxit-use-after-free-pdf-reader-vulnerabilities-found/
Fortinet warns about Critical flaw in Wireless LAN Manager FortiWLM	https://securityaffairs.com/172144/hacking/fortinet-warns-of-a-patched-fortiwlm-vulnerability.html
Hikvision Camera Driver Vulnerability Records Login details in Log files	https://cybersecuritynews.com/hikvision-camera-driver-vulnerability/
Critical Chrome Vulnerabilities Let Attackers Execute Remote Code – Update Now	https://cybersecuritynews.com/critical-chrome-vulnerabilities-patch-now/
Multiple GStreamer Vulnerabilities Impact Linux Distributions Using GNOME	https://cybersecuritynews.com/gstreamer-vulnerabilities-impact-gnome-environments/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
LockBit Admins Tease a New Ransomware Version	https://www.infosecurity-magazine.com/news/lockbit-admins-tease-a-new/
Cyberattack hits BeyondTrust Remote Support SaaS implementations	https://www.scworld.com/brief/cyberattack-hits-beyondtrust-remote-support-saas-implementations
Lazarus Group Spotted Targeting Nuclear Engineers with CookiePlus Malware	https://thehackernews.com/2024/12/lazarus-group-spotted-targeting-nuclear.html
Juniper warns of Mirai botnet scanning for Session Smart routers	https://www.bleepingcomputer.com/news/security/juniper-warns-of-mirai-botnet-scanning-for-session-smart-routers/
Campaign abusing HubSpot targets 20,000 Microsoft Azure accounts	https://www.bleepingcomputer.com/news/security/campaign-abusing-hubspot-targets-20-000-microsoft-azure-accounts/
Suspected Chinese malware operation menacing IoT devices with Hiatus RAT	https://www.scworld.com/news/suspected-chinese-malware-operation-menacing-iot-devices-with-hiatus-rat
APT29 Hackers Target High-Value Victims Using Rogue RDP Servers and PyRDP	https://thehackernews.com/2024/12/apt29-hackers-target-high-value-victims.html
Juniper Warns of Mirai Botnet Targeting SSR Devices with Default Passwords	https://thehackernews.com/2024/12/juniper-warns-of-mirai-botnet-targeting.html
Androxgh0st Botnet Targets IoT Devices, Exploiting 27 Vulnerabilities	https://hackread.com/androxgh0st-botnet-iot-devices-exploit-vulnerabilities/
Google Calendar Phishing Scam Targets Users with Malicious Invites	https://hackread.com/google-calendar-phishing-scam-users-malicious-invites/
Hackers Exploiting Linux eBPF to Spread Malware in Ongoing Campaign	https://hackread.com/hackers-exploit-linux-ebpf-malware-ongoing-campaign/
New Malware Can Kill Engineering Processes in ICS Environments	https://www.infosecurity-magazine.com/news/malware-engineering-ics/
Hackers Selling Cracked Version of Acunetix Tool as Araneida Scanner	https://cybersecuritynews.com/acunetix-tool-as-araneida-scanner/
BADBOX Botnet Hacked 74,000 Android Devices With Customizable Remote Codes	https://cybersecuritynews.com/badbox-botnet-hacked-74000-android-devices/
Beware Of Malicious SharePoint Notifications Delivering Xloader Malware	https://cybersecuritynews.com/xloader-malware-via-spoofed-sharepoint-notifications/
New DDoS Malware “cShell” Exploit Linux Tools to Attack SSH Servers	https://cybersecuritynews.com/ddos-malware-cshell-exploit-linux-tools-to-attack-ssh-servers/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
New infosec products of the week: December 20, 2024	https://www.helpnetsecurity.com/2024/12/20/new-infosec-products-of-the-week-december-20-2024/
CISA orders federal agencies to secure their Microsoft cloud environments	https://www.helpnetsecurity.com/2024/12/19/cisa-bod-25-01-directive-secure-microsoft-cloud-environments/

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.

5 Annex – Websites with vendor specific vulnerabilities

Ο πίνακας περιέχει websites από κατασκευαστές που προσφέρουν πληροφορίες σχετικές με ευπάθειες που εμφανίζονται στα προϊόντα τους.

Vendor name / Platform	URL
Wordpress	Wordfence Intelligence Vulnerability Database API https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ Scan your WordPress website, https://wpscan.com/scan/
Oracle	Critical Patch Updates, Security Alerts and Bulletins, https://www.oracle.com/security-alerts/
Fortinet	Fortinet products, https://www.fortiguard.com/psirt
IBM	Security bulletins, https://cloud.ibm.com/status/security Research, Collaborate and Act on threat intelligence, https://exchange.xforce.ibmcloud.com/
MS Windows	The Microsoft Security Response Center (MSRC), https://msrc.microsoft.com/update-guide/
SAP	SAP Security Notes, https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
Dell	Security Advisories, Notices and Resources, https://www.dell.com/support/security/en-us
HPE	HPE Security Bulletin Library, https://support.hpe.com/connect/s/securitybulletinlibrary Security Bulletins, https://support.hp.com/us-en/security-bulletins
Cisco	Cisco Security Advisories, https://sec.cloudapps.cisco.com/security/center/publicationListing.x
Palo Alto	Palo Alto Networks Security Advisories, https://security.paloaltonetworks.com/
Ivanti	Security Advisory, https://www.ivanti.com/blog/topics/security-advisory
Mozilla	Mozilla Foundation Security Advisories, https://www.mozilla.org/en-US/security/advisories/
Android	Android Security Bulletins, https://source.android.com/docs/security/bulletin/asb-overview
Zyxel	Security Advisories, https://www.zyxel.com/global/en/support/security-advisories
D-Link	Global Security Advisories, Responses, and Notices, https://supportannouncement.us.dlink.com/
Adobe	Security Bulletins and Advisories, https://helpx.adobe.com/security/security-bulletin.html
Siemens	Siemens ProductCERT and Siemens CERT, https://www.siemens.com/global/en/products/services/cert.html
Splunk	Splunk Security Advisories, https://advisory.splunk.com/