Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 03/12/2024 - 06/12/2024

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-2024-51378	10	CyberPanel (aka Cyber Panel)	bypass authenticatio n	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-2024-10905	10	IdentityIQ (Sailpoint)	Improper Access Control	8.4 and all 8.4 patch levels prior to 8.4p2 8.3 and all 8.3 patch levels prior to 8.3p5 8.2 and all 8.2 patch levels prior to 8.2p8 and all prior versions	N/A	https://www.sailpoint.com/ https://www.sailpoint.com/security-advisories/identityiq-improper-access-control-vulnerability-cve-2024-10905
https://nvd.nist.gov/vuln/detail/CVE-2024-51551	10	ABB ASPECT - Enterprise	Improper Validation of Specified Type of Input	Enterprise v3.07.02; NEXUS Series v3.07.02; MATRIX Series v3.07.02	N/A	https://library.e.abb.com/public/b7a2ed1e4f6641c4999cf875324b3b55/DS0112%20ASPECT-Enterprise.pdf?x-sign=84HI2wvqbrji8ceMI3XZggKRK+PtrvMEmDUv8RGmNRZMpItAQtzihA9zq270Z0gH https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
https://nvd.nist.gov/vuln/detail/CVE-2024-22116	9.9	Zabbix	Remote code execution	N/A	N/A	https://www.zabbix.com/ https://support.zabbix.com/browse/ZBX-25016
https://nvd.nist.gov/vuln/detail/CVE-2024-52544	9.8	Lorex products (security camera)	Out-of-bounds Write	N/A	2.800.0000000.8.R.20241111	https://www.lorex.com/fr-fr?srsltid=AfmBOopWtgd_oHgh5bgolaMtNHVS6ev6bkYSP8IJdJzr-E0tY2lI2pi8 https://www.rapid7.com/blog/post/2024/12/03/lorex-2k-indoor-wi-fi-security-camera-multiple-vulnerabilities-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2024-11680	9.8	ProjectSend	Unauthenticated Configuration Modification	prior to r1720	N/A	https://www.projectsend.org/ https://www.synacktiv.com/sites/default/files/2024-07/synacktiv-projectsend-multiple-vulnerabilities.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-40744	9.8	Joomla	Unrestricted Upload of File with Dangerous Type	before 4.4.8	N/A	https://www.joomla.org/ https://www.tassos.gr/joomla-extensions/convert-forms
https://nvd.nist.gov/vuln/detail/CVE-2024-42452	8.8	Veeam Backup & Replication	escalation of privileges	N/A	N/A	https://www.veeam.com/products/veeam-data-platform/backup-recovery.html https://www.veeam.com/kb4693

https://nvd.nist.gov/vuln/detail/CVE-2024-12053	8.8	Google Chrome	Type Confusion	prior to 131.0.6778.108	N/A	https://www.google.com/chrome/ https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-desktop.html
https://nvd.nist.gov/vuln/detail/CVE-2024-10074	8.8	OpenHarmony	Use After Free	v4.1.1 and prior	N/A	https://www.harmonyos.com/en/ https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-12.md
https://nvd.nist.gov/vuln/detail/CVE-2024-53937	8.8	Victure RX1800 WiFi 6 Router	Incorrect Authorization	EN_V1.0.0_r12_110933, hardware 1.0	N/A	https://govicture.com/ https://github.com/actuator/cve/blob/main/Victure/CVE-2024-53937.txt
https://nvd.nist.gov/vuln/detail/CVE-2024-51465	8.8	IBM App Connect Enterprise Certified Container	OS Command Injection	11.4, 11.5, 11.6, 12.0, 12.1, 12.2, and 12.3	N/A	https://www.ibm.com/support/pages/ibm-app-connect-enterprise-certified-container-versions https://www.ibm.com/support/pages/node/7177814
https://nvd.nist.gov/vuln/detail/CVE-2024-28824	8.8	Checkmk	Privilege escalation	2.3.0b4 (beta), 2.2.0p24, 2.1.0p41 and 2.0.0 (EOL)	N/A	https://checkmk.com/ https://checkmk.com/werk/16198
https://nvd.nist.gov/vuln/detail/CVE-2024-42422	8.3	Dell NetWorker,	Authorization Bypass	19.1	N/A	https://www.dell.com/en-us/lp/dt/data-protection-suite-networker-data-protection-software https://www.dell.com/support/kbdoc/en-us/000255892/dsa-2024-478-security-update-for-dell-networker-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2022-41137	8.3	Apache Hive	Deserialization of Untrusted Data	N/A	N/A	https://hive.apache.org/ https://lists.apache.org/thread/jwtr3d9yovf2wo0qlxvkhoxnwxxyzgts
https://nvd.nist.gov/vuln/detail/CVE-2024-11398	8.1	Synology Router Manager (SRM)	Path Traversal	before 1.3.1-9346-9	N/A	https://www.synology.com/en-global/srm https://www.synology.com/en-global/security/advisory/Synology_SA_24_03
https://nvd.nist.gov/vuln/detail/CVE-2024-53999	8.1	Mobile Security Framework (MobSF)	Cross-Site Scripting	N/A	N/A	https://github.com/MobSF/Mobile-Security-Framework-MobSF https://github.com/MobSF/Mobile-Security-Framework-MobSF/security/advisories/GHSA-5jc6-h9w7-jm3p
https://nvd.nist.gov/vuln/detail/CVE-2024-45106	8.1	Apache Ozone	Improper Authentication	1.4.0	N/A	https://ozone.apache.org/ https://lists.apache.org/thread/rylnxwttp004kvotpk9j158vb238pfkm
https://nvd.nist.gov/vuln/detail/CVE-2024-53703	8.1	SonicWall SMA100 SSLVPN	Stack-based Buffer Overflow	firmware 10.2.1.13-72sv and earlier	N/A	https://www.sonicwall.com/products/remote-access/secure-mobile-access-100-series https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0018
https://nvd.nist.gov/vuln/detail/CVE-2024-12149	8.1	Devolutions Remote Desktop Manager	Incorrect Permission Assignment for Critical Resource	2024.3.19.0 and earlier on Windows	N/A	https://devolutions.net/remote-desktop-manager/ https://devolutions.net/security/advisories/DEVO-2024-0017
https://nvd.nist.gov/vuln/detail/CVE-2024-54154	8	JetBrains YouTrack	Relative Path Traversal	before 2024.3.51866	N/A	https://www.jetbrains.com/youtrack/ https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2024-40691	8	IBM Cognos Controller	Unrestricted Upload of File	11.0.0 and 11.0.1	N/A	https://www.ibm.com/products/controller https://www.ibm.com/support/pages/node/7177220

https://nvd.nist.gov/vuln/detail/CVE-2024-54664	7.8	Veritas NetBackup	execution of malicious code	before 10.5	N/A	https://www.veritas.com/protection/netbackup https://www.veritas.com/content/support/en_US/security/VTS24-012
https://nvd.nist.gov/vuln/detail/CVE-2024-24906	7.6	Dell Secure Connect Gateway (SCG) Policy Manager	Stored Cross-Site Scripting	N/A	N/A	https://www.dell.com/support/manuals/en-us/secure-connect-gateway-ve/pm_5.x_ug/download-policy-manager-for-secure-connect-gateway https://www.dell.com/support/kbdoc/en-us/000222330/dsa-2024-077-security-update-for-dell-secure-connect-gateway-policy-manager-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-10567	7.5	TI WooCommerce Wishlist plugin for WordPress	Missing Authorization	all versions up to, and including, 2.9.1	N/A	https://wordpress.org/plugins/ti-woocommerce-wishlist/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0a5f2e1a-2216-4885-9b74-a08142816f2b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-11391	7.5	Advanced File Manager plugin for WordPress	Unrestricted Upload of File	all versions up to, and including, 5.2.10	N/A	https://wordpress.org/plugins/file-manager-advanced/ https://www.wordfence.com/threat-intel/vulnerabilities/id/f14a658c-1517-4af4-8bd7-c379ac07ab35?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-53916	7.5	OpenStack Neutron	incorrect ID during policy enforcement	before 25.0.1	N/A	https://wiki.openstack.org/wiki/Neutron https://security.openstack.org/ossa/OSSA-2024-005.html
https://nvd.nist.gov/vuln/detail/CVE-2024-21075	7.5	Oracle Trade Management	unauthorized access to critical data	12.2.3-12.2.13	N/A	https://www.oracle.com/scm/logistics/global-trade-management/ https://www.oracle.com/security-alerts/cpuapr2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-11148	7.5	OpenBSD	NULL Pointer Dereference	7.4 before errata 006 and 7.3 before errata 020	N/A	https://www.openbsd.org/ https://ftp.openbsd.org/pub/OpenBSD/patches/7.3/common/020_httpd.patch.sig https://ftp.openbsd.org/pub/OpenBSD/patches/7.4/common/006_httpd.patch.sig
https://nvd.nist.gov/vuln/detail/CVE-2024-11941	7.5	Drupal	Infinite Loop	from 10.2.0 before 10.2.2, from 10.1.0 before 10.1.8	N/A	https://new.drupal.org/home https://www.drupal.org/sa-core-2024-001
https://nvd.nist.gov/vuln/detail/CVE-2024-52564	7.5	I-O DATA Routers	Inclusion of Undocumented Features or Chicken Bits	UD-LT1 firmware Ver.2.1.8 and earlier and UD-LT1/EX firmware Ver.2.1.8 and earlier	N/A	https://www.iodata.jp/support/information/2024/11_ud-lt1/ https://jvn.jp/en/jp/JVN46615026/ https://www.iodata.jp/support/information/2024/11_ud-lt1/
https://nvd.nist.gov/vuln/detail/CVE-2024-51771	7.2	HPE Aruba Networking ClearPass Policy Manager	Command Injection	N/A	N/A	https://www.hpe.com/asia_pac/en/aruba-clearpass-policy-manager.html https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04761en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/CVE-2024-45205	7.1	UniFi Access Point	Improper Certificate Validation	10.17.7 and earlier	10.18.0 or later	https://ui.com/wifi https://community.ui.com/releases/UniFi-iOS-10-18-0/42f02428-544c-4626-b5b3-5ae40308edc7
https://nvd.nist.gov/vuln/detail/CVE-2024-45717	7	SolarWinds Platform	Cross-site Scripting	N/A	N/A	https://www.solarwinds.com/orion-platform https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-45717

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-24-338-01 Ruijie Reyee OS ICSA-24-338-02 Siemens RUGGEDCOM APE1808 ICSA-24-338-03 Open Automation Software ICSA-24-338-04 ICONICS and Mitsubishi Electric GENESIS64 Products ICSA-24-338-05 Fuji Electric Monitouch V-SFT ICSA-24-338-06 Fuji Electric Tellus Lite V-Simulator ICSA-22-307-01 ETIC Telecom Remote Access Server (RAS) (Update B) ICSA-24-184-03 ICONICS and Mitsubishi Electric Products (Update A) ICSA-24-340-01 AutomationDirect C-More EA9 Programming Software ICSA-24-340-02 Planet Technology Planet WGS-804HPT	https://www.cisa.gov/news-events/alerts/2024/12/03/cisa-releases-eight-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2024/12/05/cisa-releases-two-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2023-45727 North Grid Proself Improper Restriction of XML External Entity (XEE) Reference Vulnerability CVE-2024-11680 ProjectSend Improper Authentication Vulnerability CVE-2024-11667 Zyxel Multiple Firewalls Path Traversal Vulnerability CVE-2024-51378 CyberPanel Incorrect Default Permissions Vulnerability	https://www.cisa.gov/news-events/alerts/2024/12/03/cisa-adds-three-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2024/12/04/cisa-adds-one-known-exploited-vulnerability-catalog
Cisco Releases Security Updates for NX-OS Software	Cisco NX-OS Software Image Verification Bypass Vulnerability	https://www.cisa.gov/news-events/alerts/2024/12/05/cisco-releases-security-updates-nx-os-software

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
Russian hackers hijack Pakistani hackers' servers for their own attacks	https://www.bleepingcomputer.com/news/security/russian-hackers-hijack-pakistani-hackers-servers-for-their-own-attacks/
Pro-Russian Hacktivist Group Claims 6600 Attacks Targeting Europe	https://www.infosecurity-magazine.com/news/pro-russian-hacktivist-attacks/
Wyden and Schmitt Call for Investigation of Pentagon's Phone Systems	https://www.darkreading.com/endpoint-security/wyden-and-schmitt-call-for-investigation-of-the-pentagon-s-failure-to-secure-its-phone-systems-against-foreign-spies
Authorities shut down Crimenetwork, the Germany's largest crime marketplace	https://securityaffairs.com/171658/cyber-crime/german-authorities-shut-down-crimenetwork.html
ENISA Launches First State of EU Cybersecurity Report	https://www.infosecurity-magazine.com/news/enisa-launches-first-state-eu/
Authorities Take Down Criminal Encrypted Messaging Platform MATRIX	https://hackread.com/encrypted-messaging-platform-matrix-take-down/
Hackers Leveraging Cloudflare Tunnels, DNS Fast-Flux to Hide GammaDrop Malware	https://thehackernews.com/2024/12/hackers-leveraging-cloudflare-tunnels.html
Romania's election systems targeted in over 85,000 cyberattacks	https://www.bleepingcomputer.com/news/security/romanias-election-systems-targeted-in-over-85-000-cyberattacks/
Chinese Hackers Breach US Firm, Maintain Network Access for Months	https://hackread.com/chinese-hackers-breach-us-firm-network-for-months/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
China-linked APT Salt Typhoon has breached telcos in dozens of countries	https://securityaffairs.com/171692/apt/china-salt-typhoon-breached-telecommunications.html
BT unit took servers offline after Black Basta ransomware breach	https://www.bleepingcomputer.com/news/security/bt-conferencing-division-took-servers-offline-after-black-basta-ransomware-attack/
Additional MOVEit hack data from major firms exposed	https://www.scworld.com/brief/additional-moveit-hack-data-from-major-firms-exposed
Japan warns of IO-Data zero-day router flaws exploited in attacks	https://www.bleepingcomputer.com/news/security/japan-warns-of-io-data-zero-day-router-flaws-exploited-in-attacks/
New infosec products of the week: December 6, 2024	https://www.helpnetsecurity.com/2024/12/06/new-infosec-products-of-the-week-december-6-2024/
Deloitte Hacked: Over 1TB Stolen in Cyberattack	https://dailysecurityreview.com/security-spotlight/deloitte-hacked-over-1tb-stolen-in-cyberattack/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Veeam Urges Updates After Discovering Critical Vulnerability	https://www.darkreading.com/vulnerabilities-threats/veeam-urges-updates-after-discovering-critical-vulnerability
Cisco Urges Immediate Patch for Decade-Old WebVPN Vulnerability	https://hackread.com/cisco-patch-decade-old-webvpn-vulnerability/
PoC exploit for critical WhatsUp Gold RCE vulnerability released (CVE-2024-8785)	https://www.helpnetsecurity.com/2024/12/04/poc-exploit-cve-2024-8785-whatsup-gold/
Hundred of CISCO switches impacted by bootloader flaw	https://securityaffairs.com/171729/security/cisco-switches-bootloader-flaw-cve-2024-20397.html
Rockwell Automation Vulnerabilities Let Attackers Execute Remote Code	https://cybersecuritynews.com/rockwell-automation-vulnerabilities/
Critical Windows Zero-Day Vulnerability Lets Attackers Steal Users NTLM Credentials	https://cybersecuritynews.com/windows-zero-day-vulnerability/
WordPress Gutenberg Editor Vulnerability Let Attackers Inject Malicious Scripts	https://cybersecuritynews.com/wordpress-gutenberg-editor-vulnerability/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
New DroidBot Android malware targets 77 banking, crypto apps	https://www.bleepingcomputer.com/news/security/new-droidbot-android-malware-targets-77-banking-crypto-apps/
Pegasus Spyware Infections Proliferate Across iOS, Android Devices	https://www.darkreading.com/endpoint-security/pegasus-spyware-infections-ios-android-devices
Australia, Canada, New Zealand, and the U.S. warn of PRC-linked cyber espionage targeting telecom networks	https://securityaffairs.com/171644/hacking/prc-linked-cyber-espionage-telecom-networks.html
New Android spyware found on phone seized by Russian FSB	https://www.bleepingcomputer.com/news/security/new-android-spyware-found-on-phone-seized-by-russian-fsb/
Isreali NSO Group's Pegasus Spyware Detected in New Mobile Devices	https://cybersecuritynews.com/pegasus-spyware-detected-in-new-mobile-devices/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
How the Shadowserver Foundation helps network defenders with free intelligence feeds	https://www.helpnetsecurity.com/2024/12/05/piotr-kijewski-shadowserver-foundation-secure-internet/
SafeLine: Open-source web application firewall (WAF)	https://www.helpnetsecurity.com/2024/12/04/safeline-open-source-web-application-firewall-waf/ https://github.com/chaitin/SafeLine
Choosing secure and verifiable technologies	https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/cyber-supply-chains/choosing-secure-and-verifiable-technologies

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.