Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 26/11/2024 - 29/11/2024

Contents

1 Common Vulnerabilities and Exposures (CVE) 2

2 CISA/CERT-EU Alerts & Advisories 5

3 News 5

3.1 Breaches 5

3.2 Vulnerabilities and flaws 6

3.3 Potential threats / Threat intelligence 6

3.4 Guides / Tools 7

4 References 8

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-2024-11980	**10**	Billion Electric router	Missing Authentication	N/A	N/A	https://uk.billion.com/ https://www.twcert.org.tw/en/cp-139-8274-01e55-2.html
https://nvd.nist.gov/vuln/detail/CVE-2024-42327	**9.9**	Zabbix	SQL injection	N/A	N/A	https://www.zabbix.com/ https://support.zabbix.com/browse/ZBX-25623
https://nvd.nist.gov/vuln/detail/CVE-2024-20997	**9.9**	Oracle Hospitality Simphony	Elevation of privileges	19.1.0-19.5.4	N/A	https://www.oracle.com/food-beverage/restaurant-pos-systems/simphony-pos/ https://www.oracle.com/security-alerts/cpuapr2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-8672	**9.9**	Widget Options – The #1 WordPress Widget & Block Control Plugin plugin for WordPress	Remote Code Execution	all versions up to, and including, 4.0.7	N/A	https://wordpress.org/plugins/widget-options/ https://www.wordfence.com/threat-intel/vulnerabilities/id/8d03af4d-a1f9-4c15-a62e-f4cdbcfc9af7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-8932	**9.8**	PHP versions	integer overflow	8.1.* before 8.1.31, 8.2.* before 8.2.26, 8.3.* before 8.3.14	N/A	https://www.php.net/ https://github.com/php/php-src/security/advisories/GHSA-g665-fm4p-vhff https://nvd.nist.gov/vuln/detail/CVE-2024-8932 cve-icon https://www.cve.org/CVERecord?id=CVE-2024-8932
https://nvd.nist.gov/vuln/detail/CVE-2024-53676	**9.8**	Hewlett Packard Enterprise Insight Remote Support	remote code execution	N/A	N/A	https://support.hpe.com/connect/s/softwaredetails?language=en_US&collectionId=MTX-a6bba8aac84e4f46&tab=releaseNotes https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04731en_us
https://nvd.nist.gov/vuln/detail/CVE-2024-9680	**9.8**	Firefox, Thunderbird	Use-after-free	Firefox < 131.0.2, Firefox ESR < 128.3.1, Firefox ESR < 115.16.1, Thunderbird < 131.0.1, Thunderbird < 128.3.1, and Thunderbird < 115.16.0	N/A	https://www.mozilla.org/el/firefox/new/ https://www.mozilla.org/en-US/security/advisories/mfsa2024-51/ https://www.mozilla.org/en-US/security/advisories/mfsa2024-52/ https://www.mozilla.org/security/advisories/mfsa2024-51/ https://www.mozilla.org/security/advisories/mfsa2024-52/
https://nvd.nist.gov/vuln/detail/CVE-2024-11320	**9.8**	Pandora FMS	Command Injection	from 700 through <=777.4	N/A	https://pandorafms.com/en/ https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/

https://nvd.nist.gov/vuln/detail/CVE-2024-4879	9.8	ServiceNow	Jelly Template Injection	N/A	N/A	https://www.servicenow.com/ https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1645154
https://nvd.nist.gov/vuln/detail/CVE-2024-11482	9.8	Trellix (ESM)	remote code execution	11.6.10	N/A	https://www.trellix.com/products/enterprise-security-manager/ https://thrive.trellix.com/s/article/000014058#h2_0
https://nvd.nist.gov/vuln/detail/CVE-2024-5910	9.8	Palo Alto Networks Expedition	Missing Authenticatio n	N/A	N/A	https://live.paloaltonetworks.com/t5/expedition/ct-p/migration_tool https://security.paloaltonetworks.com/CVE-2024-5910
https://nvd.nist.gov/vuln/detail/CVE-2024-7971	9.6	Google Chrome V8	heap corruption	prior to 128.0.6613.84	N/A	https://www.google.com/chrome/ https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
https://nvd.nist.gov/vuln/detail/CVE-2024-39576	8.8	Dell Power Manager (DPM)	Elevation of privileges	3.15.0 and prior	N/A	https://www.dell.com/support/contents/el-gr/article/product-support/self-support-knowledgebase/software-and-downloads/dell-power-manager https://www.dell.com/support/kbdoc/en-us/000227010/dsa-2024-323
https://nvd.nist.gov/vuln/detail/CVE-2024-52899	8.5	IBM Data Virtualization Manager	inject malicious JDBC URL parameters and execute code	z/OS 1.1 and 1.2	N/A	https://www.ibm.com/products/data-virtualization-manager-for-zos https://www.ibm.com/support/pages/node/7177091
https://nvd.nist.gov/vuln/detail/CVE-2024-8114	8.2	GitLab CE/EE	Missing Authorization	all versions from 8.12 before 17.4.5, 17.5 before 17.5.3, and 17.6 before 17.6.1	N/A	https://about.gitlab.com/ https://gitlab.com/gitlab-org/gitlab/-/issues/480494 (requests account sign in)
https://nvd.nist.gov/vuln/detail/CVE-2024-11599	8.2	Mattermost	Domain Restriction Bypass on Registration	10.0.x <= 10.0.1, 10.1.x <= 10.1.1, 9.11.x <= 9.11.3, 9.5.x <= 9.5.11	N/A	https://mattermost.com/ https://mattermost.com/security-updates
https://nvd.nist.gov/vuln/detail/CVE-2024-52323	8.1	Zohocorp ManageEngine Analytics Plus	Sensitive Data Exposure	below 6100	N/A	https://www.manageengine.com/analytics-plus/ https://www.manageengine.com/analytics-plus/CVE-2024-52323.html
https://nvd.nist.gov/vuln/detail/CVE-2024-7245	7.8	Panda Security Dome VPN	Local Privilege Escalation	N/A	N/A	https://www.pandasecurity.com/en/homeusers/vpn/ https://www.zerodayinitiative.com/advisories/ZDI-24-1015/
https://nvd.nist.gov/vuln/detail/CVE-2024-38831	7.8	VMware Aria Operations	Local Privilege Escalation	N/A	N/A	https://www.vmware.com/products/cloud-infrastructure/cloud-foundation-operations https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25199
https://nvd.nist.gov/vuln/detail/CVE-2024-9852	7.8	Mitsubishi Electric GENESIS64	Malicious Code Execution	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-2024-11667	7.5	Zyxel ATP series	directory traversal	V5.00 through V5.38, USG FLEX V5.00 through V5.38, USG FLEX 50(W) V5.10 through V5.38, and USG20(W)-VPN V5.10 through V5.38	N/A	https://www.zyxel.com/global/en/products/next-gen-firewall/atp-firewall-zywall-atp500 https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-protecting-against-recent-firewall-threats-11-21-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-51569	7.5	Apache NimBLE	Lack of input sanitization	through 1.7.0	1.8.0	https://mynewt.apache.org/download/ https://lists.apache.org/thread/q0vs5rddx1lho30xnpsrvpzgxqmywnhs
https://nvd.nist.gov/vuln/detail/CVE-2024-8066	7.5	File Manager Pro – Filester plugin for WordPress	Arbitrary File Upload	all versions up to, and including, 1.8.4	N/A	https://wordpress.com/plugins/filester https://www.wordfence.com/threat-intel/vulnerabilities/id/27288836-e5d3-49fc-b1f6-319ea3b70839?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-31082	7.3	X.org server	heap-based buffer over-read	N/A	N/A	https://www.x.org/wiki/ https://www.cve.org/CVERecord?id=CVE-2024-31082
https://nvd.nist.gov/vuln/detail/CVE-2024-8190	7.2	Ivanti Cloud Services Appliance	OS command injection	4.6 Patch 518 and before	N/A	https://help.ivanti.com/ld/help/en_US/LDMS/10.0/Windows/csa-h-help.htm https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Service-Appliance-CSA-CVE-2024-8190
https://nvd.nist.gov/vuln/detail/CVE-2024-50364	7.2	Advantech products	OS Command Injection	EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1)	N/A	https://www.advantech.com/en https://www.nozominetworks.com/labs/vulnerability-advisories-cve-2024-50364
https://nvd.nist.gov/vuln/detail/CVE-2024-29014	7.1	SonicWall SMA100 NetExtender Windows	arbitrary code execution	10.2.339 and earlier	N/A	https://www.sonicwall.com/support/technical-documentation/docs/sma_100-10-2-user_guide/Content/sma-usr-using-vo-netext-user-config-install.htm https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0011

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-24-331-01 Schneider Electric PowerLogic PM55xx and PowerLogic PM8ECC ICSA-24-331-02 Schneider Electric PowerLogic P5 ICSA-24-331-03 Schneider Electric EcoStruxure Control Expert, EcoStruxure Process Expert, and Modicon M340, M580 and M580 Safety PLCs ICSA-24-331-04 Hitachi Energy MicroSCADA Pro/X SYS600 ICSA-24-331-05 Hitachi Energy RTU500 Scripting Interface ICSMA-24-200-01 Philips Vue PACS (Update A)	https://www.cisa.gov/news-events/alerts/2024/11/26/cisa-releases-six-industrial-control-systems-advisories

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
Researchers Discover "Bootkitty" – First UEFI Bootkit Targeting Linux Kernels	https://thehackernews.com/2024/11/researchers-discover-bootkitty-first.html
Cyber-Attacks Could Impact Romanian Presidential Race, Officials Claim	https://www.infosecurity-magazine.com/news/cyber-attacks-romanian-presidential/
VPN vulnerabilities, weak credentials fuel ransomware attacks	https://www.helpnetsecurity.com/2024/11/28/vpn-weak-credentials-ransomware-attacks/
New EU Commission to Unveil Healthcare Cybersecurity Plan in First 100 Days	https://www.infosecurity-magazine.com/news/eu-commission-healthcare-cyber-plan/
Chinese hackers eyeing U.S. critical infrastructure for potential conflict	https://www.scworld.com/brief/chinese-hackers-eyeing-u-s-critical-infrastructure-for-potential-conflict

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Zello urges users to reset passwords following a cyber attack	https://securityaffairs.com/171516/security/zello-urges-reset-passwords-following-cyber-attack.html

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Russian RomCom APT Group Leverages Zero-Day Flaws in Firefox and Windows	https://www.infosecurity-magazine.com/news/romcom-apt-zeroday-flaws-firefox/
ProjectSend Vulnerability Exploited in the Wild	https://www.securityweek.com/projectsend-vulnerability-exploited-in-the-wild/
New VPN Attack Demonstrated Against Palo Alto Networks, SonicWall Products	https://www.securityweek.com/new-vpn-attack-demonstrated-against-palo-alto-networks-sonicwall-products/
VMware Patches High-Severity Vulnerabilities in Aria Operations	https://www.securityweek.com/vmware-patches-high-severity-vulnerabilities-in-aria-operations/
IBM Patches RCE Vulnerabilities in Data Virtualization Manager, Security SOAR	https://www.securityweek.com/ibm-patches-rce-vulnerabilities-in-data-virtualization-manager-security-soar/
Critical Vulnerabilities Discovered in Industrial Wireless Access Point	https://www.infosecurity-magazine.com/news/critical-vulnerabilities/
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
Widespread WordPress compromise possible with critical plugin flaws	https://www.scworld.com/brief/widespread-wordpress-compromise-possible-with-critical-plugin-flaws
Microsoft Fixes AI, Cloud, and ERP Security Flaws; One Exploited in Active Attacks	https://thehackernews.com/2024/11/microsoft-fixes-ai-cloud-and-erp.html

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Russian Script Kiddie Assembles Massive DDoS Botnet	https://www.darkreading.com/cyberattacks-data-breaches/russian-script-kiddie-assembles-massive-ddos-botnet
Matrix Botnet Exploits IoT Devices in Widespread DDoS Botnet Campaign	https://thehackernews.com/2024/11/matrix-botnet-exploits-iot-devices-in.html
Phishing-as-a-Service "Rockstar 2FA" Targets Microsoft 365 Users with AiTM Attacks	https://thehackernews.com/2024/11/phishing-as-service-rockstar-2fa.html
South Korean Spies Exploit WPS Office Zero-Day	https://www.infosecurity-magazine.com/news/south-korean-spies-exploit-wps/
Sneaky Skimmer Malware Targets Magento Sites Ahead of Black Friday	https://www.darkreading.com/application-security/sneaky-skimmer-malware-magento-sites-black-friday
Attack Group APT-C-60 Targets Japan Using Trusted Platforms	https://www.infosecurity-magazine.com/news/aptc60-targets-japan-using-trusted/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Latest Multi-Stage Attack Scenarios with Real-World Examples	https://thehackernews.com/2024/11/latest-multi-stage-attack-scenarios.html
Why Small Businesses Are Prime Targets for Cyberattacks and How They Can Defend Themselves	https://infosecwriteups.com/why-small-businesses-are-prime-targets-for-cyberattacks-and-how-they-can-defend-themselves-7ae0d3e670d1
Hottest cybersecurity open-source tools of the month: November 2024	https://www.helpnetsecurity.com/2024/11/27/open-source-cybersecurity-tools-november-2024/

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.