Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 08/11/2024 - 12/11/2024

Contents

1 Common Vulnerabilities and Exposures (CVE)

CVEs						
URL ευπάθειας (NIST NVD)	**CVSSv 3**	**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-2024-20418	**10**	Cisco Unified Industrial Wireless Software for Cisco Ultra-Reliable Wireless Backhaul (URWB) Access Points	Command Injection	N/A	N/A	https://www.cisco.com/site/us/en/products/networking/industrial-wireless/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs
https://nvd.nist.gov/vuln/detail/CVE-2024-10547	**9.8**	WP Membership plugin for WordPress	Unauthenticated Arbitrary File Upload	all versions up to, and including, 1.6.2	N/A	https://wordpress.org/plugins/wp-members/ https://www.wordfence.com/threat-intel/vulnerabilities/id/664e6e2a-faa1-4609-b250-d7e94c5d5a04?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10508	**9.8**	RegistrationMagic – User Registration Plugin with Custom Registration Forms plugin for WordPress	Unauthenticated Privilege Escalation	all versions up to, and including, 6.0.2.6	N/A	https://wordpress.org/plugins/custom-registration-form-builder-with-submission-manager/ https://www.wordfence.com/threat-intel/vulnerabilities/id/c4679fa7-be6b-4f50-8cdf-ff9822794f19?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-5910	**9.8**	Palo Alto Networks Expedition	Missing Authentication Leads to Admin Account Takeover	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-2024-9486	**9.8**	Kubernetes Image Builder	default credentials	<= v0.1.37	N/A	https://image-builder.sigs.k8s.io/ https://groups.google.com/g/kubernetes-security-announce/c/UKJG-oZogfA/m/Lu1hcnHmAQAJ
https://nvd.nist.gov/vuln/detail/CVE-2024-11068	**9.8**	D-Link DSL6740C	Incorrect Use of Privileged APIs	N/A	N/A	https://setuprouter.com/router/dlink/dsl-6740u/1657.pdf https://www.twcert.org.tw/en/cp-139-8234-0514c-2.html

https://nvd.nist.gov/vuln/detail/CVE-2024-45763	9.1	Dell Enterprise SONiC OS	OS Command Injection	4.1.x, 4.2.x	N/A	https://www.dell.com/en-us/dt/networking/sonic/index.htm#scroll=off&accordion0 https://www.dell.com/support/kbdoc/en-us/000245655/dsa-2024-449-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-47460	9	PAPI (Aruba's Access Point management protocol)	Unauthenticated Command Injection	N/A	N/A	https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/papi-enha-secu/enha-secu.htm https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04722en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/CVE-2024-23309	9	LevelOne WBR-6012	authentication bypass	firmware R0.40e6	N/A	https://download.level1.info/manual/WBR-6012_UM_V1.0.pdf https://talosintelligence.com/vulnerability_reports/TALOS-2024-1996
https://nvd.nist.gov/vuln/detail/CVE-2024-11061	8.8	Tenda AC10	stack-based overflow	16.03.10.13	N/A	https://www.tendacn.com/gr/product/ac10v3.html https://tasty-foxtrot-3a8.notion.site/Tenda-AC10v4-FUN_0044db3c-stack-overflow-13a0448e619580ae96fee2899545e159
https://nvd.nist.gov/vuln/detail/CVE-2024-24409	8.8	Zohocorp ManageEngine ADManager Plus	Privilege Escalation	7203 and prior	N/A	https://www.manageengine.com/products/ad-manager/manageengine-admanager-plus-integration-with-zoho-people.html https://www.manageengine.com/products/ad-manager/admanager-kb/cve-2024-24409.html
https://nvd.nist.gov/vuln/detail/CVE-2024-47590	8.8	SAP	Incomplete Filtering of Special Elements	N/A	N/A	https://www.sap.com/greece/index.html?url_id=auto_hp_redirect_greece https://me.sap.com/notes/3520281 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2024-11048	8.8	D-Link DI-8003	Improper Restriction of Operations within the Bounds of a Memory Buffer	16.07.16A1	N/A	https://github.com/advisories/GHSA-cvj9-g4h2-mvqx https://github.com/theRaz0r/iot-mycve/blob/main/Dlink_DI8003_stackoverflow/Dlink-DI8003-stackoverflow-dbsrv.md
https://nvd.nist.gov/vuln/detail/CVE-2024-45794	8.3	evtron is an open source tool integration platform for Kubernetes	SQL Injection	N/A	0.7.2	https://devtron.ai/ https://github.com/devtron-labs/devtron/security/advisories/GHSA-q78v-cv36-8fxj
https://nvd.nist.gov/vuln/detail/CVE-2024-10006	8.3	Consul and Consul Enterprise (“Consul”)	Vulnerable To Headers Bypass	N/A	N/A	https://developer.hashicorp.com/consul/docs/enterprise https://discuss.hashicorp.com/t/hcsec-2024-23-consul-l7-intentions-vulnerable-to-headers-bypass

https://nvd.nist.gov/vuln/detail/CVE-2024-50121	7.8	Linux kernel, (nfsd) Multiple Linux kernel vulnerabilities are present	use-after-free errors	N/A	N/A	https://linux.die.net/man/7/nfsd https://lore.kernel.org/linux-cve-announce/2024110556-CVE-2024-50121-2a0a@gregkh/T
https://nvd.nist.gov/vuln/detail/CVE-2024-49560	7.8	Dell SmartFabric OS10	Command Injection	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/000247217/dsa-2024-425-security-update-for-dell-networking-os10-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-47131	7.8	Delta Electronics DIAScreen	Stack-based Buffer Overflow	N/A	N/A	https://www.deltaww.com/en-us/products/DIAStudio/5040 https://www.cisa.gov/news-events/ics-advisories/icsa-24-312-02 https://www.deltaww.com/en-US/Cybersecurity_Advisory
https://nvd.nist.gov/vuln/detail/CVE-2024-48783	7.5	Ruijie NBR3000D-E Gateway	remote attacker to obtain sensitive information	N/A	N/A	https://www.ruijienetworks.com/products/security-listing/next-generation-integrated-gateway https://gist.github.com/zty-1995/8495b81e8d257e8f6df102a32ec3c583
https://nvd.nist.gov/vuln/detail/CVE-2024-22066	7.5	ZTE ZXR10 ZSR V2	privilege escalation	N/A	N/A	https://www.zte.com.cn/global/product_index/ip_network_en/68e_e/zxr10-zsr-v2/zxr10_zsr-v2.html https://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/1171513586716225590
https://nvd.nist.gov/vuln/detail/CVE-2024-10958	7.3	WP Photo Album Plus plugin for WordPress	Unauthenticated Arbitrary Shortcode Execution	all versions up to, and including, 8.8.08.007	N/A	https://wordpress.org/plugins/wp-photo-album-plus/ https://www.wordfence.com/threat-intel/vulnerabilities/id/53bb0871-343a-4299-9902-682c422152d1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10958	7.3	WP Photo Album Plus plugin for WordPress	Code Injection	all versions up to, and including, 8.8.08.007	N/A	https://wordpress.org/plugins/wp-photo-album-plus/ https://www.wordfence.com/threat-intel/vulnerabilities/id/53bb0871-343a-4299-9902-682c422152d1?source=cve

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
2023 Top Routinely Exploited Vulnerabilities		**https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a**
CISA Releases Industrial Control Systems Advisories	ICSA-24-317-01 Subnet Solutions PowerSYSTEM Center ICSA-24-317-02 Hitachi Energy TRO600 ICSA-24-317-03 Rockwell Automation FactoryTalk View ME ICSA-23-306-03 Mitsubishi Electric MELSEC Series (Update A) ICSA-23-136-01 Snap One OvrC Cloud (Update A)	https://www.cisa.gov/news-events/alerts/2024/11/12/cisa-releases-five-industrial-control-systems-advisories

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
November 2024 Patch Tuesday forecast: New servers arrive early	https://www.helpnetsecurity.com/2024/11/11/november-2024-patch-tuesday-forecast/
After 48 Years, It's A Long Goodbye to the Diffie-Hellman Method	https://billatnapier.medium.com/after-48-years-its-a-long-goodbye-to-the-diffie-hellman-method-a6976a562bfe
The Importance of Effective Incident Response	https://hackread.com/the-importance-of-effective-incident-response/
Microsoft says recent Windows 11 updates break SSH connections	https://www.bleepingcomputer.com/news/microsoft/microsoft-says-recent-windows-11-updates-break-ssh-connections/
Preparing for DORA Amid Technical Controls Ambiguity	https://www.darkreading.com/cyber-risk/preparing-for-dora-amidst-technical-controls-ambiguity
D-Link won't fix critical flaw affecting 60,000 older NAS devices	https://www.bleepingcomputer.com/news/security/d-link-wont-fix-critical-flaw-affecting-60-000-older-nas-devices/
iPhones in a law enforcement forensics lab mysteriously rebooted losing their After First Unlock (AFU) state	https://securityaffairs.com/170683/mobile-2/iphones-in-law-enforcement-forensics-lab-mysteriously-rebooted.html
Energy Giant Halliburton Reveals $35m Ransomware Loss	https://www.infosecurity-magazine.com/news/energy-giant-halliburton-35m/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Major Oilfield Supplier Hit by Ransomware Attack	https://www.infosecurity-magazine.com/news/newpark-resources-oilfield/
Massive troves of Amazon, HSBC employee data leaked	https://www.helpnetsecurity.com/2024/11/12/amazon-employee-data-leaked/
Amazon discloses employee data breach after May 2023 MOVEit attacks	https://securityaffairs.com/170804/data-breach/amazon-employee-data-breach-may-2023-moveit-attacks.html
HIBP notifies 57 million people of Hot Topic data breach	https://www.bleepingcomputer.com/news/security/hibp-notifies-57-million-people-of-hot-topic-data-breach/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Week in review: Zero-click flaw in Synology NAS devices, Google fixes exploited Android vulnerability	https://www.helpnetsecurity.com/2024/11/10/week-in-review-zero-click-flaw-in-synology-nas-devices-google-fixes-exploited-android-vulnerability/
Mazda Connect flaws allow to hack some Mazda vehicles	https://securityaffairs.com/170727/security/mazda-connect-flaws.html
Veeam Backup & Replication exploit reused in new Frag ransomware attack	https://securityaffairs.com/170717/malware/veeam-backup-replication-flaw-frag-ransomware.html
Palo Alto Expedition bug with 9.3 rating exploited by attackers, CISA warns	https://www.scworld.com/news/palo-alto-expedition-bug-with-93-rating-exploited-by-attackers-cisa-warns
Critical NAS-ty flaw strikes D-Link storage boxes	https://www.scworld.com/news/nas-ty-flaw-strikes-d-link-storage-boxes
CISA Urges Patching of Critical Palo Alto Networks' Expedition Tool Vulnerability	https://hackread.com/cisa-patch-palo-alto-networks-expedition-tool-vulnerability/
HPE Issues Critical Security Patches for Aruba Access Point Vulnerabilities	https://thehackernews.com/2024/11/hpe-issues-critical-security-patches.html

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Cybercriminals Use Excel Exploit to Spread Fileless Remcos RAT Malware	https://thehackernews.com/2024/11/cybercriminals-use-excel-exploit-to.html

Hackers now use ZIP file concatenation to evade detection	https://www.bleepingcomputer.com/news/security/hackers-now-use-zip-file-concatenation-to-evade-detection/
Palo Alto Advises Securing PAN-OS Interface Amid Potential RCE Threat Concerns	https://thehackernews.com/2024/11/palo-alto-advises-securing-pan-os.html
Ymir ransomware, a new stealthy ransomware grow in the wild	https://securityaffairs.com/170814/malware/ymir-ransomware-analysis.html
'Top 10' malware strain, Remcos RAT, now exploiting Microsoft Excel files	https://www.scworld.com/news/excel-doc-loaded-with-remcos-rat-lets-attackers-gain-backdoor-access
Flexible Structure of Zip Archives Exploited to Hide Malware Undetected	https://www.darkreading.com/threat-intelligence/flexible-structure-zip-archives-exploited-hide-malware-undetected
Microsoft Visio Files Used in Sophisticated Phishing Attacks	https://www.infosecurity-magazine.com/news/microsoft-visio-files-phishing/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Powerpipe: Open-source dashboards for DevOps	https://www.helpnetsecurity.com/2024/11/12/powerpipe-open-source-dashboards-for-devops/

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.