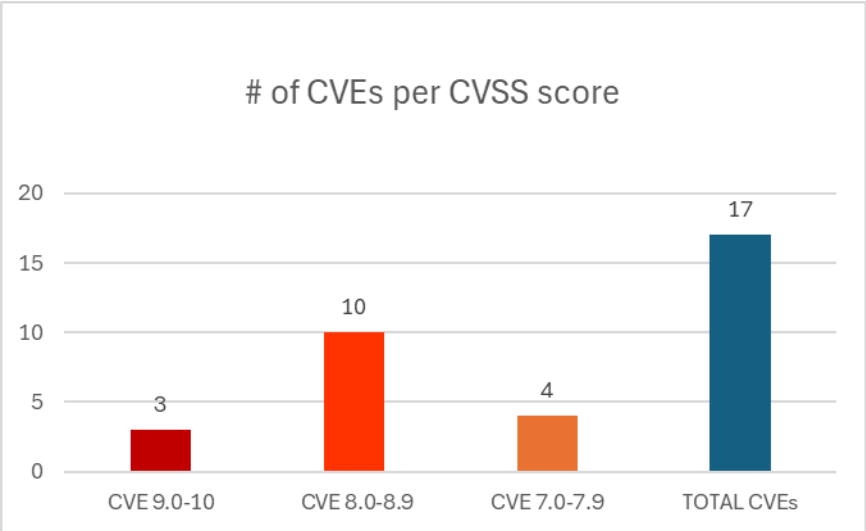
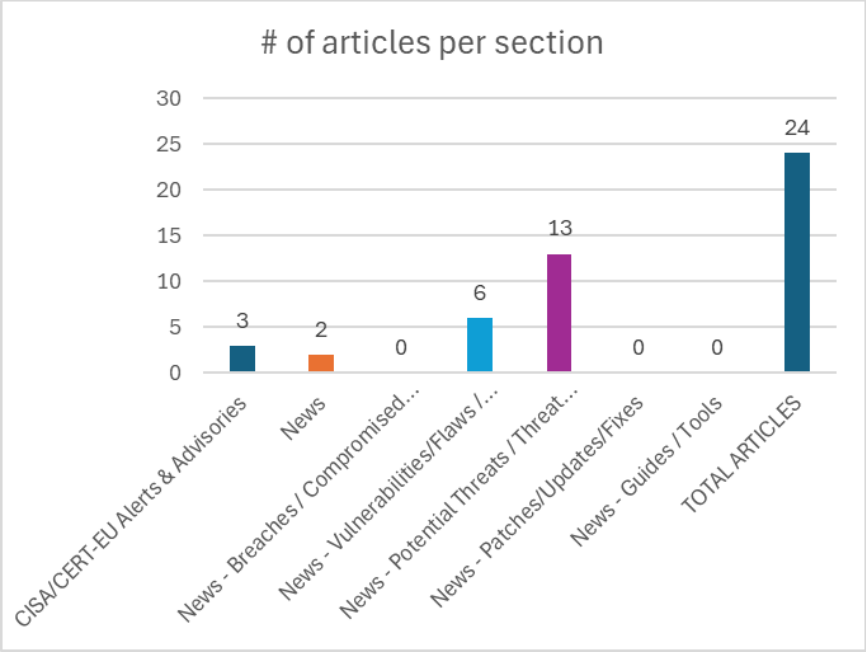
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 27/06/2025 - 01/07/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2015-0843	9,8	yubiserver	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	yubiserver before 0.6	http://www.include.gr/debian/yubiserver/#changelog https://bugs.debian.org/796495
https://nvd.nist.gov/vuln/detail/CVE-2025-3699	9,8	Mitsubishi Electric Corporation	Missing Authentication for Critical Function	Mitsubishi Electric Corporation G-50 Version 3.37 and prior, G-50-W Version 3.37 and prior, G-50A Version 3.37 and prior, GB-50 Version 3.37 and prior, GB-50A Version 3.37 and prior, GB-24A Version 9.12 and prior, G-150AD Version 3.21 and prior, AG-150A-A Version 3.21 and prior, AG-150A-J Version 3.21 and prior, GB-50AD Version 3.21 and prior, GB-50ADA-A Version 3.21 and prior, GB-50ADA-J Version 3.21 and prior, EB-50GU-A Version 7.11 and prior, EB-50GU-J Version 7.11 and prior, AE-200J Version 8.01 and prior, AE-200A Version 8.01 and prior, AE-200E Version 8.01 and prior, AE-50J Version 8.01 and prior, AE-50A Version 8.01 and prior, AE-50E Version 8.01 and prior, EW-50J Version 8.01 and prior, EW-50A Version 8.01 and prior, EW-50E Version 8.01 and prior, TE-200A Version 8.01 and prior, TE-50A Version 8.01 and prior, TW-50A Version 8.01 and prior, and CMS-RMD-J Version 1.40 and prior	https://jvn.jp/vu/JVNVU96471539/ https://www.cisa.gov/news-events/ics-advisories/icsa-25-177-01 https://www.mitsubishielectric.com/psirt/vulnerability/pdf/2025-004_en.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-45931	9,8	D-Link	Improper Neutralization of Special Elements used in a Command ('Command Injection')	D-Link DIR-816-A2 DIR-816A2_FWv1.10CNB05_R1B011D88210	http://d-link.com http://dir-816-a2.com https://github.com/Synmac05/CVE-advisories/blob/main/CVE-2025-45931.md https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2025-36593	8,8	Dell	Authentication Bypass by Capture-replay	Dell OpenManage Network Integration, versions prior to 3.8	https://www.dell.com/support/kbdoc/en-us/000337238/dsa-2025-257-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities

https://nvd.nist.gov/vuln/detail/CVE-2025-46014	8,8	Honor	Incorrect Default Permissions	Honor Device Co., Ltd Honor PC Manager v16.0.0.118	https://github.com/Souhardya/Exploit-PoCs/tree/main/HonorPCManager-PrivEsc
https://nvd.nist.gov/vuln/detail/CVE-2025-6734	8,8	UTT	Improper Restriction of Operations within the Bounds of a Memory Buffer	UTT HiPER 840G up to 3.1.1-190328	https://github.com/d2pq/cve/blob/main/616/3.md https://github.com/d2pq/cve/blob/main/616/3.md#poc https://vuldb.com/?ctiid.314009 https://vuldb.com/?id.314009 https://vuldb.com/?submit.597679
https://nvd.nist.gov/vuln/detail/CVE-2025-6751	8,8	Linksys	Improper Restriction of Operations within the Bounds of a Memory Buffer	Linksys E8450 up to 1.2.00.360516	https://github.com/CH13hh/tmp_store_cc/blob/main/E8450/1.md https://github.com/CH13hh/tmp_store_cc/blob/main/E8450/1.md#poc https://vuldb.com/?ctiid.314049 https://vuldb.com/?id.314049 https://vuldb.com/?submit.598217 https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6752	8,8	Linksys	Improper Restriction of Operations within the Bounds of a Memory Buffer	Linksys WRT1900ACS, EA7200, EA7450 and EA7500 up to 20250619	https://github.com/feiwuxingxie/cve/blob/main/linksys/vul01/1.md https://github.com/feiwuxingxie/cve/blob/main/linksys/vul01/1.md#poc https://vuldb.com/?ctiid.314050 https://vuldb.com/?id.314050 https://vuldb.com/?submit.600638 https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6824	8,8	TOTOLINK	Improper Restriction of Operations within the Bounds of a Memory Buffer	TOTOLINK X15 up to 1.0.0-B20230714.1105	https://github.com/awindog/cve/blob/main/688/28.md Exploit Third Party Advisory https://github.com/awindog/cve/blob/main/688/28.md Exploit Third Party Advisory https://github.com/awindog/cve/blob/main/688/28.md#poc Exploit Third Party Advisory https://github.com/awindog/cve/blob/main/688/28.md#poc Exploit Third Party Advisory https://vuldb.com/?ctiid.314262 Permissions Required VDB Entry https://vuldb.com/?id.314262 Third Party Advisory VDB Entry https://vuldb.com/?submit.602643 Third Party Advisory VDB Entry https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-6825	8,8	TOTOLINK	Improper Restriction of Operations within the Bounds of a Memory Buffer	TOTOLINK A702R up to 4.0.0-B20230721.1521	https://github.com/awindog/cve/blob/main/688/29.md https://github.com/awindog/cve/blob/main/688/29.md https://github.com/awindog/cve/blob/main/688/29.md#poc https://github.com/awindog/cve/blob/main/688/29.md#poc https://vuldb.com/?ctiid.314263 https://vuldb.com/?id.314263 https://vuldb.com/?submit.602655 https://www.totolink.net/

https://nvd.nist.gov/vuln/detail/CVE-2025-6882	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-513 1.0	https://vuldb.com/?ctiid.314361 https://vuldb.com/?id.314361 https://vuldb.com/?submit.603693 https://vuldb.com/?submit.603693 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6887	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC5 15.03.06.47	https://lavender-bicycle-a5a.notion.site/Tenda-AC5-fromSetSysTime_time-21d53a41781f8002bdb3fe8344d6fd8c?source=copy_link https://lavender-bicycle-a5a.notion.site/Tenda-AC5-fromSetSysTime_timeZone-21d53a41781f8021ae2fd2ac639f1b3f?source=copy_link https://vuldb.com/?ctiid.314366 https://vuldb.com/?id.314366 https://vuldb.com/?submit.603788 https://vuldb.com/?submit.603789 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-6916	8,8	TOTOLINK	Improper Authentication	TOTOLINK T6 4.1.5cu.748_B20211015	https://github.com/c0nyy/IoT_vuln/blob/main/TOTOLINK%20T6%20Vuln.md https://github.com/c0nyy/IoT_vuln/blob/main/TOTOLINK%20T6%20Vuln.md https://vuldb.com/?ctiid.314409 https://vuldb.com/?id.314409 https://vuldb.com/?submit.605101 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2024-53621	7,5	Tenda	Stack-based Buffer Overflow	Tenda AC1206 1200M 11ac US_AC1206V1.0RTL_V15.03.06.23_multi_TD01	https://drive.google.com/file/d/1b7DlkG7XVmJmCxDrX7u1X7CAk-lOv-iBX/view?usp=sharing https://github.com/qingwei4/Router-VR/blob/main/CVE-2024-53621/CVE-2024-53621.md
https://nvd.nist.gov/vuln/detail/CVE-2025-1991	7,5	IBM	Integer Underflow (Wrap or Wraparound)	IBM Informix Dynamic Server 12.10,14.10, and15.0	https://www.ibm.com/support/pages/node/7238455
https://nvd.nist.gov/vuln/detail/CVE-2025-45851	7,5	Hikvision		Hikvision DS-2CD1321-I V5.7.21 build 230819	https://assets.hikvision.com/prd/public/all/files/202506/release-note%5CNetwork_Camera-V5.7.23_SP2_Release_Note-E8.pdf https://crashpark.weebly.com/blog/hikvision-ip-camera-unauthenticated-denial-of-service-dos https://www.hikvision.com/en/support/download/firmware/

https://nvd.nist.gov/vuln/detail/CVE-2025-36595	7,2	Dell	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')	Dell Unisphere for PowerMax vApp, version(s) 9.2.4.x	https://www.dell.com/support/kbdoc/en-us/000337554/dsa-2025-235-dell-powermaxos-dell-powermax-eem-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-unisphere-360-dell-solutions-enabler-and-dell-solutions-enabler-virtual-appliance-security-update-for-multiple-vulnerabilit

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA and Partners Urge Critical Infrastructure to Stay Vigilant in the Current Geopolitical Environment		https://www.cisa.gov/news-events/alerts/2025/06/30/cisa-and-partners-urge-critical-infrastructure-stay-vigilant-current-geopolitical-environment
CISA Adds One Known Exploited Vulnerability to Catalog		https://www.cisa.gov/news-events/alerts/2025/06/30/cisa-adds-one-known-exploited-vulnerability-catalog
Vulnerability Summary for the Week of June 23, 2025		https://www.cisa.gov/news-events/bulletins/sb25-181

News

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Teams Automatically Set Work Locations Based on Organization's Wi-Fi Network	https://cybersecuritynews.com/microsoft-teams-employees-work-locations/
Windows 11 Retires Blue Screen of Death Error Replaces With Black Screen	https://cybersecuritynews.com/windows-retires-blue-screen-of-death-error/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Linux Sudo chroot Vulnerability Enables Hackers to Elevate Privileges to Root	https://cybersecuritynews.com/linux-sudo-chroot-vulnerability/
Chrome 0-Day Vulnerability Exploited in the Wild to Execute Arbitrary Code – Patch Now	https://cybersecuritynews.com/chrome-0-day-vulnerability-exploited/
Multiple Critical Vulnerabilities in D-Link Routers Let Attackers Execute Arbitrary Code Remotely	https://cybersecuritynews.com/critical-d-link-routers-vulnerabilities/
2100+ Citrix Servers Vulnerable to Actively Exploited Bypass Authentication Vulnera-bility	https://cybersecuritynews.com/2100-citrix-servers-vulnerable/
Bluetooth Vulnerabilities Let Hackers Spy on Your Headphones and Earbuds	https://cybersecuritynews.com/bluetooth-vulnerabilities/
Mitsubishi Electric AC Systems Vulnerability Allows Remote Control Without User Interaction	https://cybersecuritynews.com/mitsubishi-electric-ac-systems-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Hackers Exploiting Critical Langflow Vulnerability to Deploy Flodrix Botnet and Take System Control	https://cybersecuritynews.com/hackers-exploiting-critical-langflow-vulnerability/
Threat Actors Weaponizing Facebook Ads to Deliver Malware and Stealing Wallet Passwords	https://cybersecuritynews.com/threat-actors-weaponizing-facebook-ads/
Germany Urges Apple, Google to Block Chinese AI App DeepSeek Over Privacy Rules	https://cybersecuritynews.com/germany-urges-apple-google-to-block-chinese-ai-app-deepseek/
Zig Strike – An Offensive Toolkit to Create Payloads and Bypass AV, XDR/EDR Detections	https://cybersecuritynews.com/zig-strike/
RansomHub Ransomware Attacking RDP Servers Using Mimikatz and Advanced IP Scanner Tools	https://cybersecuritynews.com/ransomhub-ransomware-rdp-servers/
ESET Warns of NFC Data for Contactless Payments Emerges as Cybercrime Target	https://cybersecuritynews.com/eset-warns-of-nfc-data-for-contactless-payments/
Threat Actors Exploiting Windows & Linux Servers Vulnerability to Deploy Web Shell	https://cybersecuritynews.com/threat-actors-exploiting-windows-linux-servers-vulnerability/
Beware of Trending TikTok Videos That Promotes Pirated Apps Deliver Stealer Malware	https://cybersecuritynews.com/beware-of-trending-tiktok-videos-that-promotes-pirated-apps/
Weaponized DeepSeek Installers Delivers Sainbox RAT and Hidden Rootkit	https://cybersecuritynews.com/weaponized-deepseek-installers-delivers-sainbox-rat/
Cybercriminals Leveraging CapCut Popularity to Harvest Apple ID Credentials & Credit Card Data	https://cybersecuritynews.com/cybercriminals-leveraging-capcut-popularity/
Threat Actors Embed Malware on Windows System's Task Scheduler to Maintain Persistence	https://cybersecuritynews.com/threat-actors-embed-malware-on-windows-systems-task-scheduler/
ClickFix Attack Emerges by Over 500% – Hackers Actively Using This Technique to Trick Users	https://cybersecuritynews.com/clickfix-attack-emerges-by-over-500/
APT-C-36 Hackers Attacking Government Institutions, Financial Organizations, and Critical Infrastructure	https://cybersecuritynews.com/apt-c-36-hackers-attacking-government-institutions/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL

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.

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/