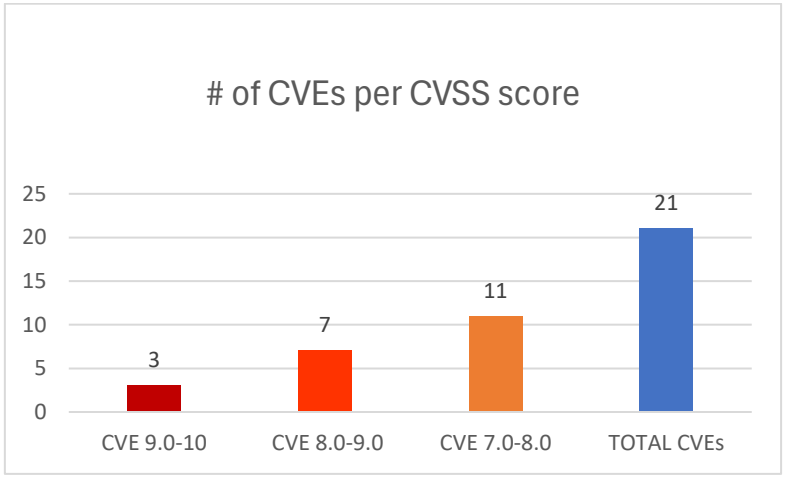
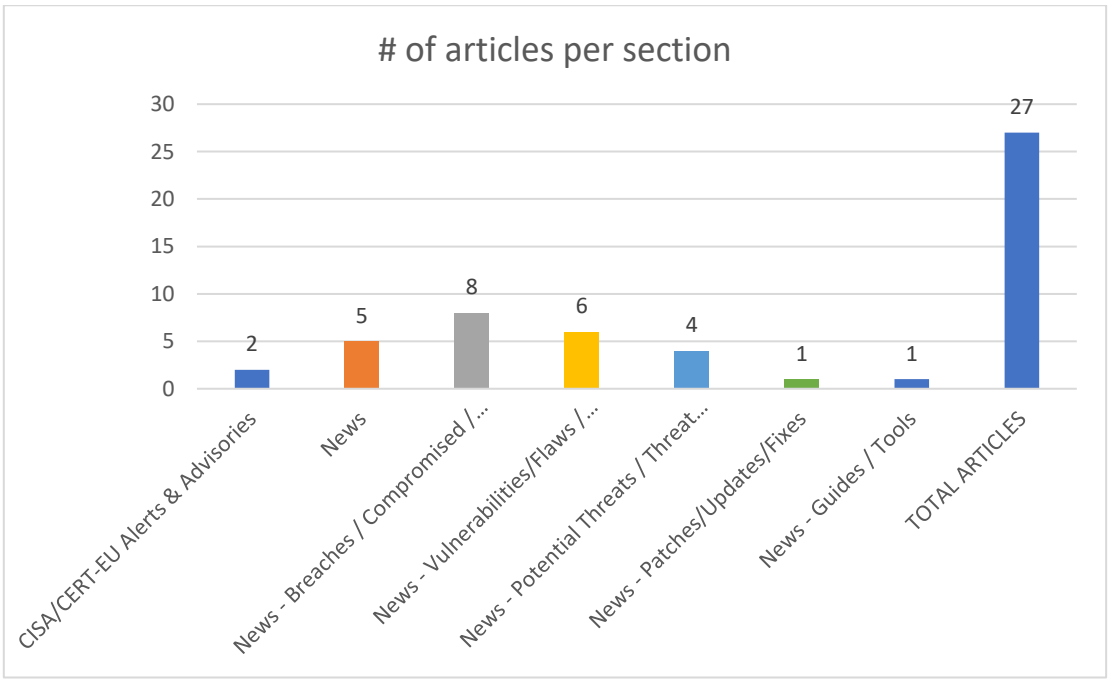
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 21/06/2025 - 24/06/2025





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 7
News 7
Breaches / Compromised / Hacked 8
Vulnerabilities / Flaws / Zero-day 8
Patches / Updates / Fixes 9
Potential threats / Threat intelligence 9
Guides / Tools 9
References 10
Annex – Websites with vendor specific vulnerabilities 11

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-2025-52562	10,0	Convoy	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	versions 3.9.0-rc3 to before 4.4.1	https://github.com/ConvoyPanel/panel/commit/f8d6202f3e4912b65dbd9f80ba625576944ab36c https://github.com/ConvoyPanel/panel/security/advisories/GHSA-43g3-qpwq-hfgg
https://nvd.nist.gov/vuln/detail/CVE-2024-45347	9,6	Xiaomi Mi Connect Service APP	Improper Authentication		https://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=548
https://nvd.nist.gov/vuln/detail/CVE-2025-6513	9,3	BRAIN2	Password in Configuration File		https://www.bizerba.com/downloads/global/information-security/2025/bizerba-sa-2025-0003.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-6367	8,8	D-Link DIR-619L 2.06B01	Stack-based Buffer Overflow		https://github.com/wudipjq/my_vuln/blob/main/D-Link6/vuln_67/67.md https://vuldb.com/?ctiid.313360 https://vuldb.com/?id.313360 https://vuldb.com/?submit.597420 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6399	8,8	TOTOLINK	Improper Restriction of Operations within the Bounds of a Memory Buffer	X15 1.0.0-B20230714.1105	https://github.com/d2pq/cve/blob/main/616/19.md https://github.com/d2pq/cve/blob/main/616/19.md#poc https://vuldb.com/?ctiid.313392 https://vuldb.com/?id.313392 https://vuldb.com/?submit.597681 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-41427	8,8	WRH-733GBK and WRH-733GWH	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	WRH-733GBK and WRH-733GWH	https://jvn.jp/en/jp/JVN39435597/ https://www.elecom.co.jp/news/security/20250624-02/

https://nvd.nist.gov/vuln/detail/CVE-2025-49126	8,8	Visionatrix	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	In versions 1.5.0 to before 2.5.1	https://github.com/Visionatrix/Visionatrix/commit/63aafe6e4d1bffe4bf69e73b6fdfc65c71a8f5b8 https://github.com/Visionatrix/Visionatrix/security/advisories/GHSA-w36r-9jvx-q48v
https://nvd.nist.gov/vuln/detail/CVE-2025-6511	8,8	Netgear	Stack-based Buffer Overflow	EX6150 1.0.0.46_1.0.76	https://github.com/xiaobor123/vul-finds/tree/main/vul-find-ex6150-netgear https://github.com/xiaobor123/vul-finds/tree/main/vul-find-ex6150-netgear#poc https://vuldb.com/?ctiid.313623 https://vuldb.com/?id.313623 https://vuldb.com/?submit.595999 https://vuldb.com/?submit.596008 https://www.netgear.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-52488	8,6	DNN (formerly DotNetNuke)	Exposure of Sensitive Information to an Unauthorized Actor	versions 6.0.0 to before 10.0.1	https://github.com/dnnsoftware/Dnn.Platform/security/advisories/GHSA-mgfv-2362-jq96
https://nvd.nist.gov/vuln/detail/CVE-2025-2828	8,4	RequestsToolkit	Server-Side Request Forgery (SSRF)	langchain-ai/langchain version 0.0.27	https://github.com/langchain-ai/langchain/commit/e188d4ecb085d4561a0be3c583d26aa9c2c3283f https://huntr.com/bounties/8f771040-7f34-420a-b96b-5b93d4a99afc
https://nvd.nist.gov/vuln/detail/CVE-2025-52922	7,4	Innoshop	Relative Path Traversal	through 0.4.1	https://github.com/innocommerce/innoshop https://medium.com/@The_Hiker/how-i-found-multiple-cves-in-innoshop-0-4-1-12c8f84ad87f
https://nvd.nist.gov/vuln/detail/CVE-2025-27387	7,4	OPPO Clone Phone	Exposure of Sensitive Information to an Unauthorized Actor		https://security.oppo.com/en/noticeDetail?notice_only_key=NOTICE-1937080145974403072https://
https://nvd.nist.gov/vuln/detail/CVE-2025-6364	7,3	Simple Pizza Ordering System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/rom4j/cve/issues/6 https://vuldb.com/?ctiid.313357 https://vuldb.com/?id.313357 https://vuldb.com/?submit.597305

https://nvd.nist.gov/vuln/detail/CVE-2025-6394	7,3	Simple Online Hotel Reservation System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/aoc1997/cve/issues/1 https://vuldb.com/?ctiid.313387 https://vuldb.com/?id.313387 https://vuldb.com/?submit.597662
https://nvd.nist.gov/vuln/detail/CVE-2025-6406	7,3	Campcodes Online Hospital Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/ASantsSec/CVE/issues/11 https://vuldb.com/?ctiid.313400 https://vuldb.com/?id.313400 https://vuldb.com/?submit.598204 https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6405	7,3	Campcodes Online Teacher Record Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/ASantsSec/CVE/issues/14 https://vuldb.com/?ctiid.313399 https://vuldb.com/?id.313399 https://vuldb.com/?submit.598200 https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6446	7,3	Client Details System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/kakalalaww/CVE/issues/18 https://vuldb.com/?ctiid.313553 https://vuldb.com/?id.313553 https://vuldb.com/?submit.598499
https://nvd.nist.gov/vuln/detail/CVE-2025-6471	7,3	Online Bidding System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/ganzhi-qcy/cve/issues/11 https://vuldb.com/?ctiid.313579 https://vuldb.com/?id.313579 https://vuldb.com/?submit.599402
https://nvd.nist.gov/vuln/detail/CVE-2025-6474	7,3	**Inventory Management System**	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/1609624781/cve/issues/1 https://vuldb.com/?ctiid.313582 https://vuldb.com/?id.313582 https://vuldb.com/?submit.600494

https://nvd.nist.gov/vuln/detail/CVE-2025-6489	7,3	Agri-Trading Online Shopping System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/ltranquility/CVE/issues/13 https://itsourcecode.com/ https://vuldb.com/?ctiid.313600 https://vuldb.com/?id.313600 https://vuldb.com/?submit.601190
https://nvd.nist.gov/vuln/detail/CVE-2025-49144	7,3	Notepad++	Incorrect Default Permissions	versions 8.8.1 and prior	https://drive.google.com/drive/folders/11yeUSWgqHvt4Bz5jO3ilRRfcpQZ6Gvpn https://github.com/notepad-plus-plus/notepad-plus-plus/commit/f2346ea00d5b4d907ed39d8726b38d77c8198f30 https://github.com/notepad-plus-plus/notepad-plus-plus/security/advisories/GHSA-9vx8-v79m-6m24

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2023-0386 Linux Kernel Improper Ownership Management Vulnerability	https://www.cisa.gov/news-events/alerts/2025/06/17/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Five Industrial Control Systems Advisories	▪ ICSA-25-168-01 Siemens Mendix Studio Pro ▪ ICSA-25-168-02 LS Electric GMWin 4 ▪ ICSA-25-168-04 Fuji Electric Smart Editor ▪ ICSA-25-168-05 Dover Fueling Solutions ProGauge MagLink LX Consoles ▪ ICSA-24-347-10 Siemens SENTRON Powercenter 1000 (Update A)	https://www.cisa.gov/news-events/alerts/2025/06/17/cisa-releases-five-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
Iran confirmed it shut down internet to protect the country against cyberattacks	https://securityaffairs.com/179199/cyber-warfare-2/iran-confirmed-it-shut-down-internet-to-protect-the-country-against-cyberattacks.html
Cloudflare blocks record 7.3 Tbps DDoS attack against hosting provider	https://www.bleepingcomputer.com/news/security/cloudflare-blocks-record-73-tbps-ddos-attack-against-hosting-provider/
Google Adds Multi-Layered Defenses to Secure GenAI from Prompt Injection Attacks	https://thehackernews.com/2025/06/google-adds-multi-layered-defenses-to.html
Aflac discloses breach amidst Scattered Spider insurance attacks	https://www.bleepingcomputer.com/news/security/aflac-discloses-breach-amidst-scattered-spider-insurance-attacks/
DHS Warns of Rise in Cyberattacks in Light of US-Iran Conflict	https://www.darkreading.com/threat-intelligence/dhs-cyberattacks-iran-conflict

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
BitoPro exchange links Lazarus hackers to $11 million crypto heist	https://www.bleepingcomputer.com/news/security/bitopro-exchange-links-lazarus-hackers-to-11-million-crypto-heist/?&web_view=true
Tonga Ministry of Health hit with cyberattack affecting website, IT systems	https://therecord.media/tonga-ministry-of-health-hit-with-cyberattack?&web_view=true
Ransomware gang says it stole confidential files from Taos County, NM; demands ransom in 7 days	https://www.comparitech.com/news/ransomware-gang-says-it-stole-confidential-files-from-taos-county-nm-demands-ransom-in-7-days/?&web_view=true
16 Billion Passwords Leaked in the Biggest Breach Ever — Change Yours NOW	https://infosecwriteups.com/16-billion-passwords-leaked-in-the-biggest-breach-ever-change-yours-now-17a66f805b6f?source=collection_home
Fake Web3 Wallet Prompt Steals $43,000 from CoinMarketCap Users	https://www.infosecurity-magazine.com/news/web3-wallet-prompt-steals-43000/
McLaren Health Care says data breach impacts 743,000 patients	https://www.bleepingcomputer.com/news/security/mclaren-health-care-says-data-breach-impacts-743-000-patients/
Russian dairy supply disrupted by cyberattack on animal certification system	https://therecord.media/russia-dairy-supply-disrupted-cyberattack?&web_view=true
Oxford City Council suffers breach exposing two decades of data	https://www.bleepingcomputer.com/news/security/oxford-city-council-suffers-breach-exposing-two-decades-of-data/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
WordPress Motors theme flaw mass-exploited to hijack admin accounts	https://www.bleepingcomputer.com/news/security/wordpress-motors-theme-flaw-mass-exploited-to-hijack-admin-accounts/
Critical OpenVPN Driver Vulnerability Allows Attackers to Crash Windows Systems	https://cybersecuritynews.com/openvpn-driver-vulnerability/
NCSC Warns of 'UMBRELLA STAND' Malware Attacking Fortinet FortiGate Firewalls	https://cybersecuritynews.com/ncsc-warns-of-umbrella-stand-malware/
XDigo Malware Exploits Windows LNK Flaw in Eastern European Government Attacks	https://thehackernews.com/2025/06/xdigo-malware-exploits-windows-lnk-flaw.html
Notepad++ Vulnerability Let Attacker Gain Complete System Control – PoC Released	https://cybersecuritynews.com/notepad-vulnerability/
Amazon EKS Vulnerabilities Expose Sensitive AWS Credentials and Escalate Privileges	https://cybersecuritynews.com/amazon-eks-vulnerabilities/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Citrix Patches Critical Vulns in NetScaler ADC and Gateway	https://www.darkreading.com/vulnerabilities-threats/citrix-patches-vulns-netscaler-adc-gateway

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Threat Actor Allegedly Selling FortiGate API Exploit Tool Targeting FortiOS	https://cybersecuritynews.com/fortigate-api-exploit-tool/
Violence-as-a-Service: Encrypted Apps Used in Recruiting Teens as Hitmen	https://hackread.com/violence-as-a-service-encrypted-apps-recruit-teen-hitmen/
New SparkKitty Malware Attacks iOS and Android Devices in Wild Via App Store and Google Play	https://cybersecuritynews.com/sparkkitty-ios-and-android-devices/
WhatsApp Banned on U.S. House Staffers Devices Due to Potential Security Risks	https://cybersecuritynews.com/whatsapp-banned/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/

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/