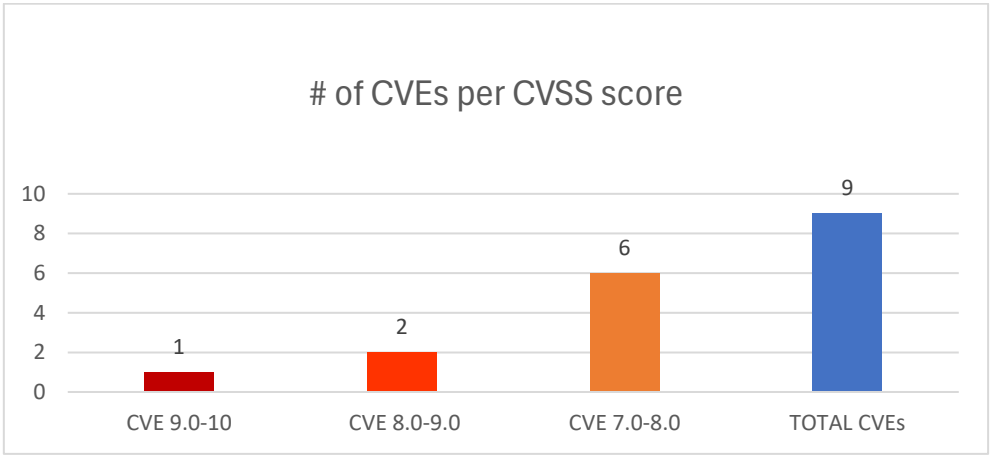
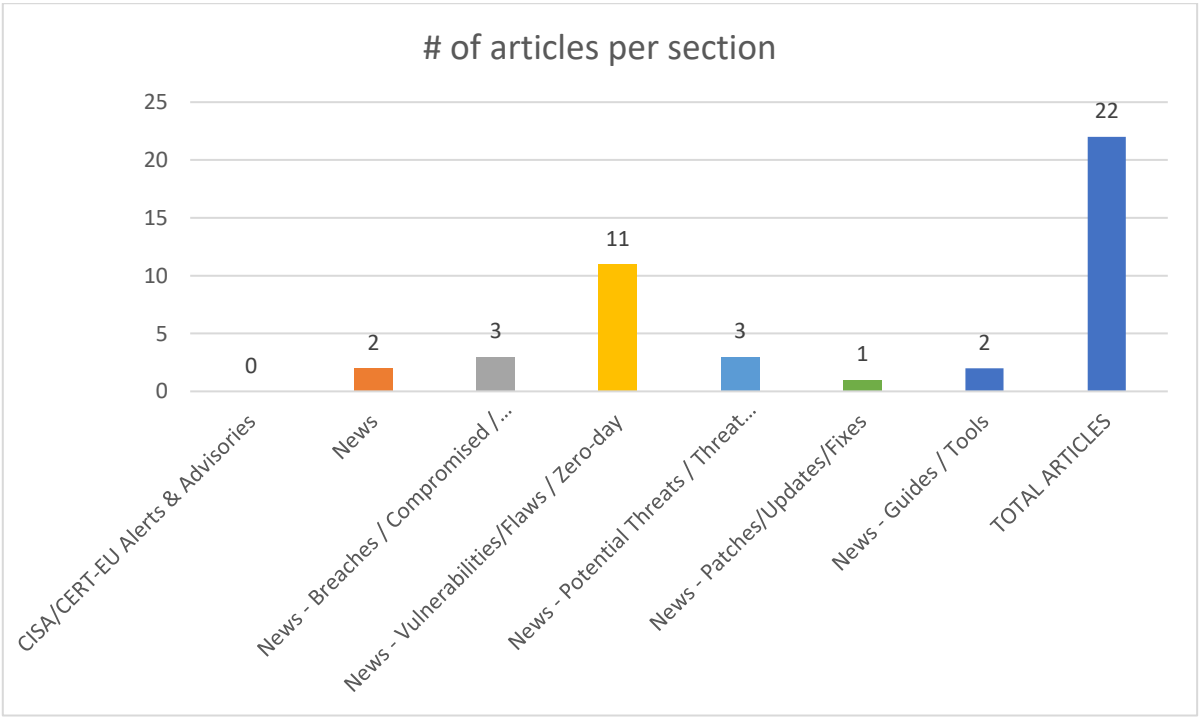
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 09/08/2025 - 12/08/2025





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 5
News 5
Breaches / Compromised / Hacked 5
Vulnerabilities / Flaws / Zero-day 5
Patches / Updates / Fixes 6
Potential threats / Threat intelligence 6
Guides / Tools 6
References 7
Annex – Websites with vendor specific vulnerabilities 8

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-2025-55013	10,0	The Assemblyline 4 Service Client	Relative Path Traversal	versions below 4.6.1.dev138	https://github.com/CybercentreCanada/assemblyline-service-client/commit/351414e7e96cc1f5640ae71ae51b939e8ba30900 GitHub, Inc. https://github.com/CybercentreCanada/assemblyline/security/advisories/GHSA-75jv-vfxf-3865\
https://nvd.nist.gov/vuln/detail/CVE-2025-8819	8,8	Linksys	Stack-based Buffer Overflow	RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801	https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_53/53.md VulDB https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_53/53.md#poc VulDB https://vuldb.com/?ctiid.319353 VulDB https://vuldb.com/?id.319353 VulDB https://vuldb.com/?submit.626683 VulDB https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-8810	8,8	Tenda	Stack-based Buffer Overflow	AC20 16.03.08.05	https://github.com/LaiwanHundun/CVE/blob/main/cve1 VulDB https://vuldb.com/?ctiid.319339 VulDB https://vuldb.com/?id.319339 VulDB https://vuldb.com/?submit.627394 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-8798	7,8	oitcode samarium	Improper Access Control	up to 0.9.6	https://github.com/MaiqueSilva/VulnDB/blob/main/readme08.md VulDB https://vuldb.com/?ctiid.319326 VulDB https://vuldb.com/?id.319326 VulDB https://vuldb.com/?submit.626077
https://nvd.nist.gov/vuln/detail/CVE-2025-8811	7,3	Simple Art Gallery	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/Darlingzero2/cve/issues/3 VulDB https://vuldb.com/?ctiid.319340 VulDB https://vuldb.com/?id.319340 VulDB https://vuldb.com/?submit.627395

https://nvd.nist.gov/vuln/detail/CVE-2025-8773	7,3	Dinstar Monitoring Platform 甘肃省危险品库监控平台	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/qiantx/cve/blob/main/cve6.md VulDB https://vuldb.com/?ctiid.319296 VulDB https://vuldb.com/?id.319296 VulDB https://vuldb.com/?submit.625361
https://nvd.nist.gov/vuln/detail/CVE-2025-8752	7,3	wangzhixuan spring-shiro-training	Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 94812c1fd8f7fe796c931f4984ff1aa0671ab562	https://gitee.com/wangzhixuan/spring-shiro-training/issues/ICP2ME CISA-ADP, VulDB https://vuldb.com/?ctiid.319246 VulDB https://vuldb.com/?id.319246 VulDB https://vuldb.com/?submit.623679
https://nvd.nist.gov/vuln/detail/CVE-2025-8744	7,3	CesiumLab Web	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to 4.0	https://vuldb.com/?ctiid.319240 VulDB https://vuldb.com/?id.319240 VulDB https://vuldb.com/?submit.616911
https://nvd.nist.gov/vuln/detail/CVE-2025-8758	7,0	TRENDnet	Incorrect Privilege Assignment	TEW-822DRE FW103B02	https://vuldb.com/?ctiid.319263 VulDB https://vuldb.com/?id.319263 VulDB https://vuldb.com/?submit.624299 VulDB https://www.notion.so/23e54a1113e78009adc9d909b254812b

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
-	-	-

News

Σύντομη περιγραφή / Τίτλος	URL
Over 29,000 Exchange servers unpatched against high-severity flaw	https://www.bleepingcomputer.com/news/security/over-29-000-exchange-servers-unpatched-against-high-severity-flaw/
Microsoft tests cloud-based Windows 365 disaster recovery PCs	https://www.bleepingcomputer.com/news/microsoft/microsoft-tests-cloud-based-windows-365-disaster-recovery-pcs/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Connex Credit Union Breach Exposes 172,000 Members' Data	https://www.infosecurity-magazine.com/news/connex-credit-union-breach/
NCSC Warns of Citrix Netscaler Vulnerability CVE-2025-6543 Exploited to Breach Orgs	https://cybersecuritynews.com/ncsc-warns-of-citrix-netscaler-vulnerability/
CastleLoader Malware Infected Over 400+ Devices Using Cloudflare-Themed ClickFix Phishing Attack	https://cybersecuritynews.com/castleloader-malware-infected-over-400-devices/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Researchers Spot Surge in Erlang/OTP SSH RCE Exploits, 70% Target OT Firewalls	https://thehackernews.com/2025/08/researchers-spot-surge-in-erlangotp-ssh.html
WinRAR Zero-Day Under Active Exploitation – Update to Latest Version Immediately	https://thehackernews.com/2025/08/winrar-zero-day-under-active.html
DarkBit Hackers Attacking VMware ESXi Servers to Deploy Ransomware and Encrypt VMDK Files	https://cybersecuritynews.com/darkbit-hackers-attacking-vmware-esxi-servers/
Smart Bus Systems Vulnerability Let Hackers Remotely Track and Control Vehicles	https://cybersecuritynews.com/smart-bus-systems-vulnerability/
Netherlands: Citrix Netscaler flaw CVE-2025-6543 exploited to breach orgs	https://www.bleepingcomputer.com/news/security/netherlands-citrix-netscaler-flaw-cve-2025-6543-exploited-to-breach-orgs/
Linux-Based Lenovo Webcams' Flaw Can Be Remotely Exploited for BadUSB Attacks	https://thehackernews.com/2025/08/linux-based-lenovo-webcams-flaw-can-be.html
ChatGPT Connectors '0-click' Vulnerability Let Attackers Exfiltrate Data From Google Drive	https://cybersecuritynews.com/chatgpt-0-click-connectors-vulnerability/
Darknet Market Escrow Systems is Vulnerable to Administrator Exit Scams	https://cybersecuritynews.com/darknet-market-escrow-systems-is-vulnerable-to-administrator-exit-scams/

CyberArk and HashiCorp Flaws Enable Remote Vault Takeover Without Credentials	https://thehackernews.com/2025/08/cyberark-and-hashicorp-flaws-enable.html
Xerox FreeFlow Vulnerabilities leads to SSRF and RCE Attacks	https://cybersecuritynews.com/xerox-freeflow-vulnerabilities/
New Win-DDoS Flaws Let Attackers Turn Public Domain Controllers into DDoS Botnet via RPC, LDAP	https://thehackernews.com/2025/08/new-win-ddos-flaws-let-attackers-turn.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
What the Matter 1.4.2 update means for smart home security	https://www.helpnetsecurity.com/2025/08/11/matter-1-4-2-smart-home-security/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Hackers Using ClickFix Technique to Attack Windows Machine and Execute Powershell Commands	https://cybersecuritynews.com/hackers-using-clickfix-technique-to-attack-windows-machine/
Threat Actors Using Typosquatted PyPI Packages to Steal Cryptocurrency from Bittensor Wallets	https://cybersecuritynews.com/typosquatted-pypi-packages-steal-from-bittensor-wallets/
Silent Watcher Attacking Windows Systems and Exfiltrate Data Using Discord Webhook	https://cybersecuritynews.com/silent-watcher-attacking-windows-systems/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/
10 Best Vulnerability Management Tools In 2025	https://cybersecuritynews.com/vulnerability-management-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.

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/