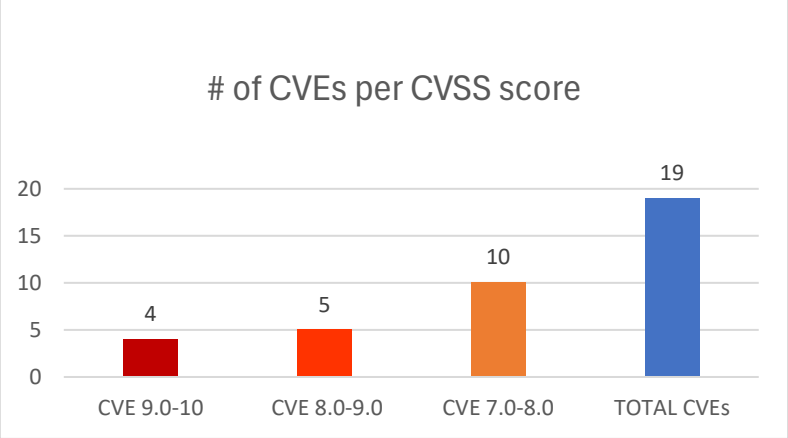
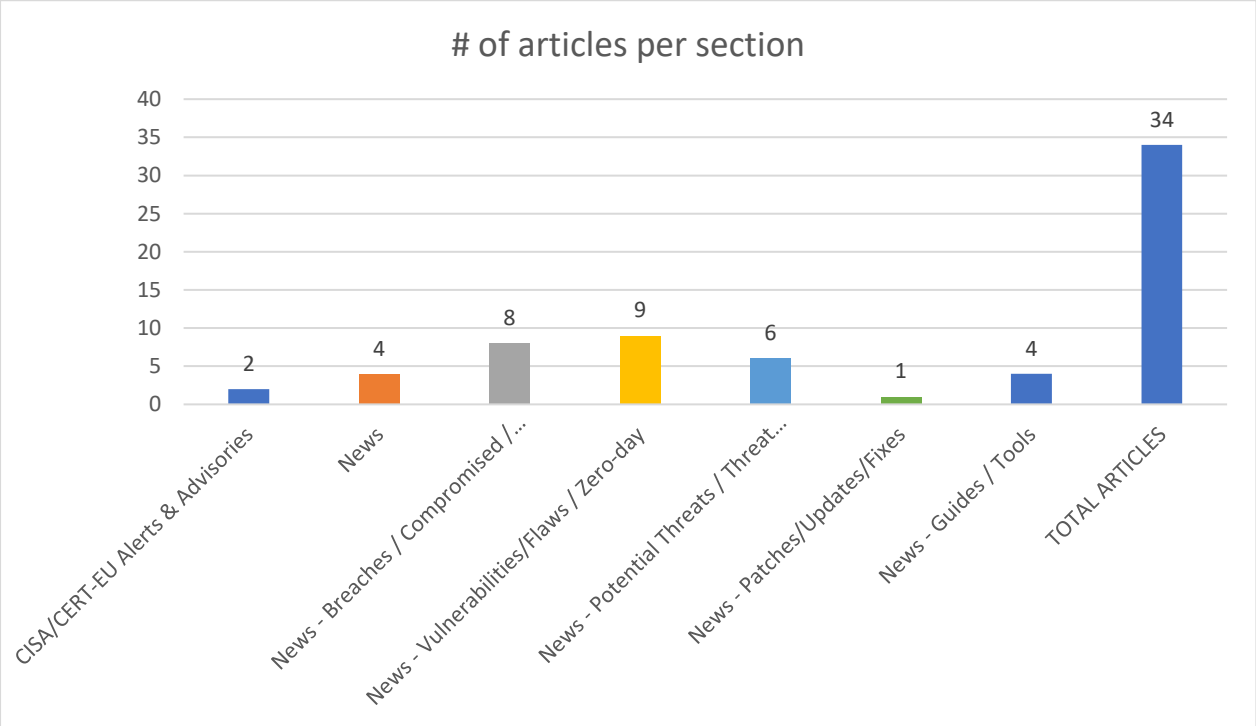
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 27/08/2025 - 29/08/2025





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-2025-22408	9,8	rfc_check_send_cmd of rfc_utils.cc	Use After Free		https://android.googlesource.com/platform/packages/modules/Bluetooth/+/806774b1cf641e0c0e7df8024e327febf23d7d7c Android (associated with Google Inc. or Open Handset Alliance) https://source.android.com/security/bulletin/2025-03-01
https://nvd.nist.gov/vuln/detail/CVE-2025-9523	9,8	Tenda	Stack-based Buffer Overflow	AC1206 15.03.06.23	https://github.com/XXRicardo/iot-cve/blob/main/Tenda/AC1206/AC1206V1.0RTL_V15.03.06.23.md VulDB https://vuldb.com/?ctiid.321541 VulDB https://vuldb.com/?id.321541 VulDB https://vuldb.com/?submit.634309 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-52122	9,8	Freeform	Improper Control of Generation of Code ('Code Injection')	5.0.0 to before 5.10.16	https://github.com/TimTrademark/CVE-2025-52122 MITRE https://github.com/TimTrademark/CVE-CraftCMS-Freeform
https://nvd.nist.gov/vuln/detail/CVE-2025-43728	9,6	Dell ThinOS 10	Protection Mechanism Failure	versions prior to 2508_10.0127	https://www.dell.com/support/kbdoc/en-us/000359619/dsa-2025-331
https://nvd.nist.gov/vuln/detail/CVE-2025-22411	8,8	process_service_attr_rsp of sdp_discovery.cc	Use After Free		https://android.googlesource.com/platform/packages/modules/Bluetooth/+/806774b1cf641e0c0e7df8024e327febf23d7d7c Android (associated with Google Inc. or Open Handset Alliance) https://source.android.com/security/bulletin/2025-03-01

https://nvd.nist.gov/vuln/detail/CVE-2025-9525	8,8	Linksys	Stack-based Buffer Overflow	E1700 1.0.0.4.003	https://github.com/wudipjq/my_vuln/blob/main/Linksys2/vuln_58/58.md VulDB https://github.com/wudipjq/my_vuln/blob/main/Linksys2/vuln_58/58.md#poc VulDB https://vuldb.com/?ctiid.321542 VulDB https://vuldb.com/?id.321542 VulDB https://vuldb.com/?submit.634824 VulDB https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-50989	8,8	OPNsense	Improper Neutralization of Special Elements used in a Command ('Command Injection')	25.1	https://github.com/4rdr/proofs/blob/main/info/OPNsense-25.1-Command-Injection-via-span-parameter.md
https://nvd.nist.gov/vuln/detail/CVE-2025-22404	8,4	avct_lcb_msg_ind of avct_lcb_act.cc	Use After Free		https://android.googlesource.com/platform/packages/modules/Bluetooth/+/806774b1cf641e0c0e7df8024e327febf23d7d7c Android (associated with Google Inc. or Open Handset Alliance) https://source.android.com/security/bulletin/2025-03-01
https://nvd.nist.gov/vuln/detail/CVE-2025-50983	8,3	GET /api/v1/wanted/cutoff API endpoint	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	readarr 0.4.15.2787	https://github.com/4rdr/proofs/blob/main/info/readarr-0.4.15.2787-sql-injection-via-sortkey-parameter.md
https://nvd.nist.gov/vuln/detail/CVE-2025-57797	7,8	ScanSnap Manager	Incorrect Privilege Assignment	versions prior to V6.5L61	https://jvn.jp/en/jp/JVN69684540/ JPCERT/CC https://www.pfu.ricoh.com/imaging/news/news20230606.html JPCERT/CC https://www.pfu.ricoh.com/scansnap/software/sshome/requirement.html
https://nvd.nist.gov/vuln/detail/CVE-2025-0093	7,5	handleBondStateChanged of AdapterService.java	Incorrect Permission Assignment for Critical Resource		https://android.googlesource.com/platform/packages/modules/Bluetooth/+/090ca53cc13c12e3763777a6a3c7367641e9808f Android (associated with Google Inc. or Open Handset Alliance) https://source.android.com/security/bulletin/2025-03-01
https://nvd.nist.gov/vuln/detail/CVE-2025-35114	7,5	Agiloft Release 28	Use of Default Credentials		https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2025/va-25-239-01.json Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian

					Government https://wiki.agiloft.com/display/HELP/What%27s+New%3A+CVE+Resolution Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government https://www.cve.org/CVERecord?id=CVE-2025-35114
https://nvd.nist.gov/vuln/detail/CVE-2025-53105	7,5	Gestionnaire Libre de Parc Informatique	Improper Privilege Management	10.0.0 to before 10.0.19	https://github.com/glpi-project/glpi/releases/tag/10.0.19 GitHub, Inc. https://github.com/glpi-project/glpi/security/advisories/GHSA-334r-2682-95wc
https://nvd.nist.gov/vuln/detail/CVE-2025-20241	7,4	Cisco NX-OS Software for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches	Compiler Optimization Removal or Modification of Security-critical Code		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n39k-isis-dos-JhJA8Rfx
https://nvd.nist.gov/vuln/detail/CVE-2025-9502	7,3	Campcodes Online Loan Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/skyrainoh/CVE/issues/10 CISA-ADP, VulDB https://vuldb.com/?ctiid.321485 VulDB https://vuldb.com/?id.321485 VulDB https://vuldb.com/?submit.635353 VulDB https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-9507	7,3	Apartment Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/zzb1388/cve/issues/47 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.321503 VulDB https://vuldb.com/?id.321503 VulDB https://vuldb.com/?submit.635387
https://nvd.nist.gov/vuln/detail/CVE-2025-9529	7,3	Campcodes Payroll Management System	External Control of File Name or Path	1.0	https://github.com/chenjunjie3/cve/issues/6 VulDB https://vuldb.com/?ctiid.321548 VulDB https://vuldb.com/?id.321548 VulDB https://vuldb.com/?submit.635551 VulDB https://www.campcodes.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-9533	7,3	TOTOLINK	Improper Authentication	T10 4.1.8cu.5241 _B20210927	https://github.com/aL-tEr6/MY_test/blob/main/TOTOLINK/TOTOLINK%20T10%20Vulnerability.md CISA-ADP, VulDB https://vuldb.com/?ctiid.321552 VulDB https://vuldb.com/?id.321552 VulDB https://vuldb.com/?submit.635941 VulDB https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-20317	7,1	Virtual Keyboard Video Monitor (vKVM) connection handling of Cisco Integrated Management Controller (IMC)	URL Redirection to Untrusted Site ('Open Redirect')		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-vkvmorv-CnKrV7HK

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Nine Industrial Control Systems Advisories	▪ **ICSA-25-240-01** Mitsubishi Electric MELSEC iQ-F Series CPU Module ▪ **ICSA-25-240-02** Mitsubishi Electric MELSEC iQ-F Series CPU Module ▪ **ICSA-25-240-03** Schneider Electric Saitel DR & Saitel DP Remote Terminal Unit ▪ **ICSA-25-240-04** Delta Electronics CNCSoft-G2 ▪ **ICSA-25-240-05** Delta Electronics COMMGR ▪ **ICSA-25-240-06** GE Vernova CIMPLICITY ▪ **ICSA-24-135-04** Mitsubishi Electric Multiple FA Engineering Software Products (Update D) ▪ **ICSA-25-140-04** Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update B) ▪ **ICSA-25-184-01** Hitachi Energy Relion 670/650 and SAM600-IO series (Update A)	**https://www.cisa.gov/news-events/alerts/2025/08/28/cisa-releases-nine-industrial-control-systems-advisories**
CISA and Partners Release Joint Advisory on Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems		**https://www.cisa.gov/news-events/alerts/2025/08/27/cisa-and-partners-release-joint-advisory-countering-chinese-state-sponsored-actors-compromise**

News

Σύντομη περιγραφή / Τίτλος	URL
ENISA to Coordinate €36m EU-Wide Incident Response Scheme	**https://www.infosecurity-magazine.com/news/enisa-coordinate-36m-euwide/**
CISA Strengthens Software Procurement Security With New Tool	https://www.infosecurity-magazine.com/news/cisa-software-procurement-security/
200 Swedish municipalities impacted by a major cyberattack on IT provider	**https://securityaffairs.com/181668/security/200-swedish-municipalities-impacted-by-a-major-cyberattack-on-it-provider.html**
Dutch intelligence warn that China-linked APT Salt Typhoon targeted local critical infrastructure	https://securityaffairs.com/181677/apt/dutch-intelligence-warns-that-china-linked-apt-salt-typhoon-targeted-local-critical-infrastructure.html

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Google Warns Salesloft OAuth Breach Extends Beyond Salesforce, Impacting All Integrations	https://thehackernews.com/2025/08/google-warns-salesloft-oauth-breach.html
TransUnion Data Breach Impacts 4.5 Million US Customers	https://www.infosecurity-magazine.com/news/transunion-data-breach-us-customers/
Ransomware group says it hacked West Chester Township, OH	https://www.comparitech.com/news/ransomware-group-says-it-hacked-west-chester-township-oh/?&web_view=true
The Salvation Army notifies victims of data breach that leaked Social Security numbers	https://www.comparitech.com/news/the-salvation-army-notifies-victims-of-data-breach-that-leaked-social-security-numbers/?&web_view=true
Nx Packages With Millions of Weekly Downloads Hacked With Credential Stealer Malware	https://cybersecuritynews.com/nx-packages-hacked/
MathWorks Confirms Cyberattack, User Personal Information Stolen	https://cybersecuritynews.com/mathworks-confirms-cyberattack/
Farmers Insurance Cyber Attack – 1.1 Million Customers Data Exposed in Salesforce Attack	https://cybersecuritynews.com/farmers-insurance-cyber-attack/
Netherlands Confirms China's Salt Typhoon Targeted Small Dutch Telcos	https://www.infosecurity-magazine.com/news/china-salt-typhoon-dutch-telcos/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
FreePBX Servers Targeted by Zero-Day Flaw, Emergency Patch Now Available	https://thehackernews.com/2025/08/freepbx-servers-targeted-by-zero-day.html
Silver Fox APT Hackers Leveraging Vulnerable driver to Attack Windows 10 and 11 Systems by Evading EDR/AV	https://cybersecuritynews.com/silver-fox-apt-hackers-leveraging-vulnerable-driver/
Nagios XSS Vulnerability Let Remote Attackers to Execute Arbitrary JavaScript	https://cybersecuritynews.com/nagios-xss-vulnerability/
Over 28,000 Citrix devices vulnerable to new exploited RCE flaw	https://www.bleepingcomputer.com/news/security/over-28-200-citrix-instances-vulnerable-to-actively-exploited-rce-bug/
Malicious VS Code Extensions Exploit Name Reuse Loophole	https://www.infosecurity-magazine.com/news/vs-code-extensions-exploit-name/
IPFire Web-Based Firewall Interface Allows Authenticated Administrator to Inject Persistent JavaScript	https://cybersecuritynews.com/ipfire-web-based-firewall-interface-flaw/
Cisco Nexus 3000 and 9000 Series Vulnerability Let Attackers Trigger DoS Attack	https://cybersecuritynews.com/cisco-nexus-3000-and-9000-series-vulnerability/
Cisco IMC Virtual Keyboard Video Monitor Let Attacker Direct User to Malicious Website	https://cybersecuritynews.com/cisco-imc-vulnerability/
PhpSpreadsheet Library Vulnerability Enables Attackers to Feed Malicious HTML Input	https://cybersecuritynews.com/phpspreadsheet-library-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Citrix Patches Three NetScaler Flaws, Confirms Active Exploitation of CVE-2025-7775	https://thehackernews.com/2025/08/citrix-patches-three-netscaler-flaws.html

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Hackers Target Popular Nx Build System in First AI-Weaponized Supply Chain Attack	https://www.securityweek.com/hackers-target-popular-nx-build-system-in-first-ai-weaponized-supply-chain-attack/
ShadowSilk Leveraging Penetration-Testing Tools, Public Exploits to Attack Organizations	https://cybersecuritynews.com/shadowsilk-attacking-penetration-testing-tools/
New Mac Malware Dubbed 'JSCoreRunner' Weaponizing PDF Conversion Site to Deliver Malware	https://cybersecuritynews.com/new-mac-malware-dubbed-jscorerunner/
Hackers Abuse Microsoft Teams to Gain Remote Access on Windows With PowerShell-based Malware	https://cybersecuritynews.com/microsoft-teams-for-remote-access/
Someone Created the First AI-Powered Ransomware Using OpenAI's gpt-oss:20b Model	https://thehackernews.com/2025/08/someone-created-first-ai-powered.html
Weaponized ScreenConnect RMM Tool Tricks Users into Downloading Xworm RAT	https://cybersecuritynews.com/screenconnect-rmm-tool/

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/
Top 15 Best Security Incident Response Tools In 2025	https://cybersecuritynews.com/incident-response-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-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/