NATIONAL CYBERSECURITY AUTHORITY GR

CVEs Alerts

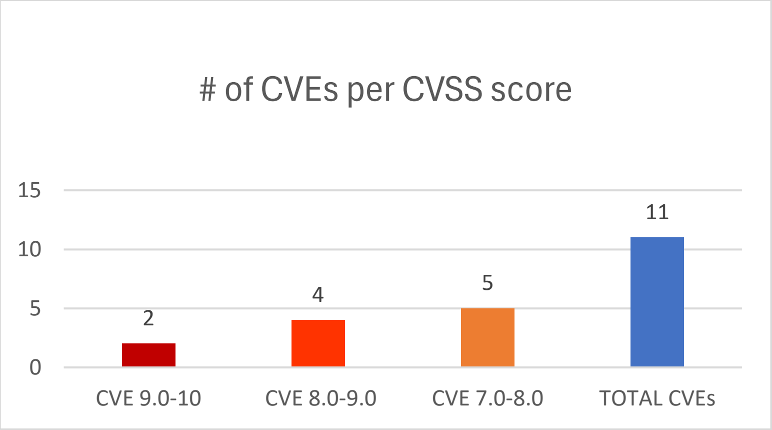
CVEs, CISA/CERT-EU Alerts Advisories & News

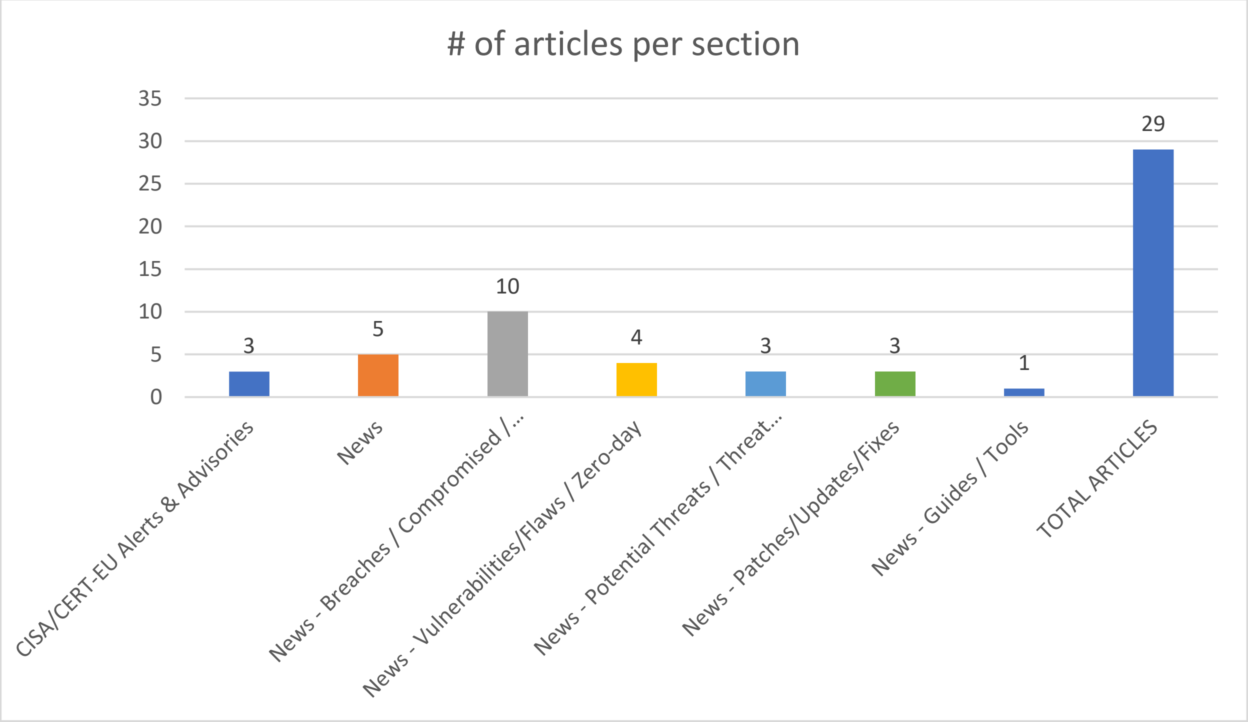
Newsletter on system vulnerabilities and cybersecurity news

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 16/07/2025 - 18/07/2025





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-2025-6222	9.8	The WooCommerce Refund And Exchange with RMA - Warranty Management, Refund Policy, Manage User Wallet theme for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 3.2.6	https://codecanyon.net/item/woocommerce-refund-and-exchange/17810207#item-description__changelog https://www.wordfence.com/threat-intel/vulnerabilities/id/35a7b5a1-b052-4390-8e08-f97aa9c16b29?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7643	9.1	The Attachment Manager plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 2.1.2	https://wordpress.org/plugins/attachment-manager/ https://www.wordfence.com/threat-intel/vulnerabilities/id/5731b971-4408-4c64-809c-e95fba33009e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-6718	8.8	The B1.lt plugin for WordPress	Missing Authorization	all versions up to, and including, 2.2.56	https://wordpress.org/plugins/b1-accounting/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4e479a3f-ef1a-4476-89e1-86d0f388f2c3?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7758	8.8	TOTOLINK	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	T6 up to 4.1.5cu.748_B20211015	https://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/3.md https://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/3.md#poc https://vuldb.com/?ctiid.316748 https://vuldb.com/?id.316748 https://vuldb.com/?submit.615734 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-7762	8.8	D-Link	Stack-based Buffer Overflow	DI-8100 16.07.26A1	https://github.com/XiDP0/MyCVE/blob/main/CVE/D-Link%20DI_8100-16.07.26A1/menu_nat_more_asp/menu_nat_more_asp.md https://vuldb.com/?ctiid.316757 https://vuldb.com/?id.316757 https://vuldb.com/?submit.615796 https://www.dlink.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-3740	8.8	The School Management System for Wordpress plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 93.1.0	https://codecanyon.net/item/school-management-system-for-wordpress/11470032#item-description__update-history https://www.wordfence.com/threat-intel/vulnerabilities/id/3604aece-5e76-4e8e-9caf-f518d6001277?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-6231	7.8	Lenovo Vantage	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	-	https://support.lenovo.com/us/en/product_security/LEN-196648
https://nvd.nist.gov/vuln/detail/CVE-2025-0886	7.8	Elliptic Labs Virtual Lock Sensor	Incorrect Default Permissions	-	https://support.lenovo.com/us/en/product_security/LEN-182738
https://nvd.nist.gov/vuln/detail/CVE-2025-7735	7.5	The Hospital Information System developed by UNIMAX	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	-	https://www.twcert.org.tw/en/cp-139-10249-5d48c-2.html https://www.twcert.org.tw/tw/cp-132-10248-f429e-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-7764	7.3	Online Appointment Booking System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://code-projects.org/ https://github.com/jaynewboy/cve/issues/2 https://vuldb.com/?ctiid.316764 https://vuldb.com/?id.316764 https://vuldb.com/?submit.616175
https://nvd.nist.gov/vuln/detail/CVE-2025-7757	7.3	PHPGurukul Land Record System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/hex31415926/cve/issues/4 https://phpgurukul.com/ https://vuldb.com/?ctiid.316747 https://vuldb.com/?id.316747 https://vuldb.com/?submit.615705

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Three Industrial Control Systems Advisories	▪ **ICSA-25-198-01** Leviton AcquiSuite and Energy Monitoring Hub ▪ **ICSMA-25-198-01** Panoramic Corporation Digital Imaging Software ▪ **ICSA-24-191-05** Johnson Controls Inc. Software House C●CURE 9000 (Update B)	https://www.cisa.gov/news-events/alerts/2025/07/17/cisa-releases-three-industrial-control-systems-advisories
Panoramic Corporation Digital Imaging Software		https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-198-01
Leviton AcquiSuite and Energy Monitoring Hub		https://www.cisa.gov/news-events/ics-advisories/icsa-25-198-01

News

Σύντομη περιγραφή / Τίτλος	URL
Chinese Cyber-Espionage Group Infiltrates Army National Guard Network Across the US	https://dailysecurityreview.com/security-spotlight/chinese-cyber-espionage-group-infiltrates-army-national-guard-network-across-the-us/
Most European Financial Firms Still Lagging on DORA Compliance	https://www.infosecurity-magazine.com/news/european-financial-dora-compliance/
Louis Vuitton says regional data breaches tied to same cyberattack	https://www.bleepingcomputer.com/news/security/louis-vuitton-says-regional-data-breaches-tied-to-same-cyberattack/
Cloudflare says 1.1.1.1 outage not caused by attack or BGP hijack	https://www.bleepingcomputer.com/news/security/cloudflare-says-1111-outage-not-caused-by-attack-or-bgp-hijack/
Retail Ransomware Attacks Jump 58% Globally in Q2 2025	https://www.infosecurity-magazine.com/news/retail-ransomware-jump-globally-q2/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Citrix Bleed 2 exploited weeks before PoCs as Citrix denied attacks	https://www.bleepingcomputer.com/news/security/citrix-bleed-2-exploited-weeks-before-pocs-as-citrix-denied-attacks/
SonicWall SMA devices hacked with OVERSTEP rootkit tied to ransomware	https://www.bleepingcomputer.com/news/security/sonicwall-sma-devices-hacked-with-overstep-rootkit-tied-to-ransomware/
Over 5.4 Million Affected in Healthcare Data Breach at Episource	https://www.infosecurity-magazine.com/news/54-million-affected-episource/
New Fortinet FortiWeb hacks likely linked to public RCE exploits	https://www.bleepingcomputer.com/news/security/new-fortinet-fortiweb-hacks-likely-linked-to-public-rce-exploits/
Scattered Spider-Attack Hits Co-op, Exposes Data of 6.5 Million Members	https://dailysecurityreview.com/security-spotlight/scattered-spider-attack-hits-co-op-exposes-data-of-6-5-million-members/

Co-op confirms data of 6.5 million members stolen in cyberattack	https://www.bleepingcomputer.com/news/security/co-op-confirms-data-of-65-million-members-stolen-in-cyberattack/
Chinese hackers breached National Guard to steal network configurations	https://www.bleepingcomputer.com/news/security/chinese-hackers-breached-national-guard-to-steal-network-configurations/
Hacker steals $27 million in BigONE exchange crypto breach	https://www.bleepingcomputer.com/news/security/hacker-steals-27-million-in-bigone-exchange-crypto-breach/
Google sues to disrupt BadBox 2.0 botnet infecting 10 million devices	https://www.bleepingcomputer.com/news/security/google-sues-to-disrupt-badbox-20-botnet-infecting-10-million-devices/
Massive Data Leak at Texas Adoption Agency Exposes 1.1 Million Records	https://hackread.com/massive-data-leak-texas-adoption-agency-million-records/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
CVE-2025-27210 & CVE-2025-27209: Two high-severity vulnerabilities in Node.js threaten Windows apps and hash-based services	https://infosecwriteups.com/cve-2025-27210-cve-2025-27209-two-high-severity-vulnerabilities-in-node-js-9134ea00dc2a?source=collection_home
Cisco Warns of Critical ISE Flaw Allowing Unauthenticated Attackers to Execute Root Code	https://thehackernews.com/2025/07/cisco-warns-of-critical-ise-flaw.html
Update Google Chrome to fix actively exploited zero-day (CVE-2025-6558)	https://www.helpnetsecurity.com/2025/07/16/update-google-chrome-to-fix-actively-exploited-zero-day-cve-2025-6558/
CVE-2025-6554 marks the fifth actively exploited Chrome Zero-Day patched by Google in 2025	https://securityaffairs.com/180001/hacking/cve-2025-6554-marks-the-fifth-actively-exploited-chrome-zero-day-patched-by-google-in-2025.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
VMware fixes four ESXi zero-day bugs exploited at Pwn2Own Berlin	https://www.bleepingcomputer.com/news/security/vmware-fixes-four-esxi-zero-day-bugs-exploited-at-pwn2own-berlin/
Google fixes actively exploited sandbox escape zero day in Chrome	https://www.bleepingcomputer.com/news/security/google-fixes-actively-exploited-sandbox-escape-zero-day-in-chrome/
UNC6148 Backdoors Fully-Patched SonicWall SMA 100 Series Devices with OVERSTEP Rootkit	https://thehackernews.com/2025/07/unc6148-backdoors-fully-patched.html

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Malware-as-a-Service Campaign Exploits GitHub to Deliver Payloads	https://www.infosecurity-magazine.com/news/maas-campaign-github-payloads/
Chinese Hackers Target Taiwan's Semiconductor Sector with Cobalt Strike, Custom Backdoors	https://thehackernews.com/2025/07/chinese-hackers-target-taiwans.html
Hackers Leverage Microsoft Teams to Spread Matanbuchus 3.0 Malware to Targeted Firms	https://thehackernews.com/2025/07/hackers-leverage-microsoft-teams-to.html

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.

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/