NATIONAL CYBERSECURITY AUTHORITY

CVEs Alerts

CVEs,
CISA/CERT-EU
Alerts
Advisories
& News

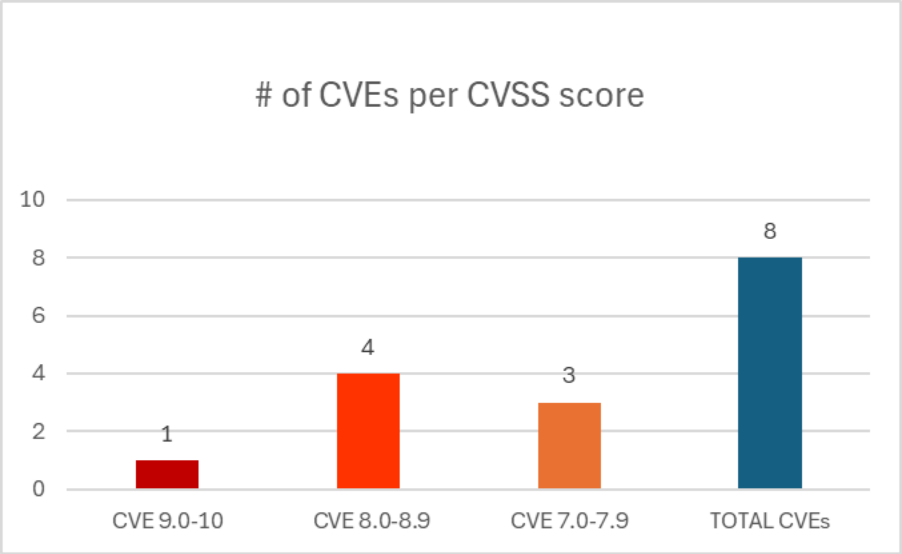
18/04/2025 -22/04/2025

Newsletter on system vulnerabilities and cybersecurity news

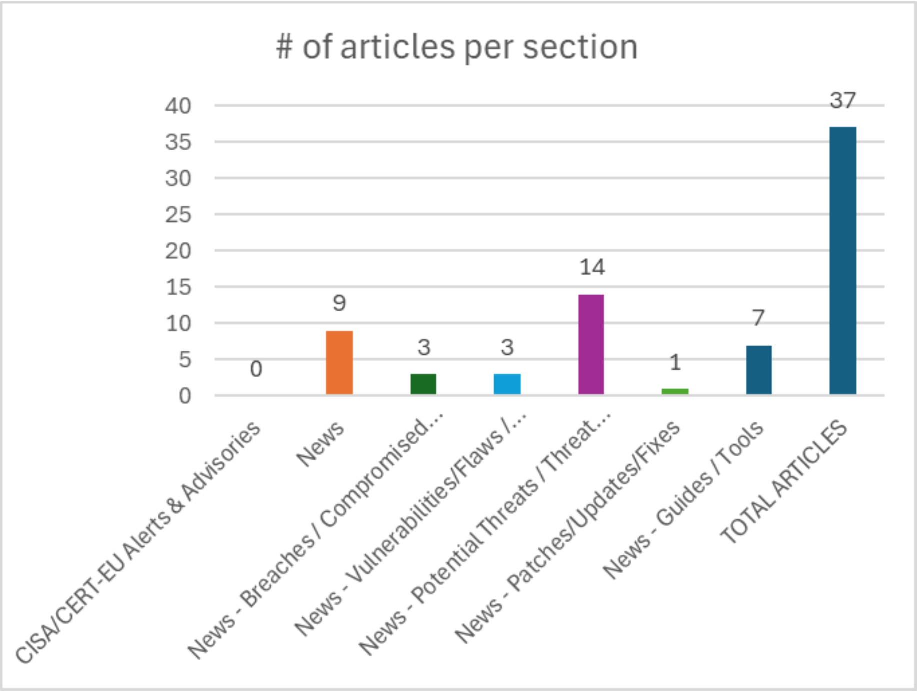
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/04/2025 - 22/04/2025



# of CVEs per CVSS score



# of articles per section

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-2021-4455	9,8	The Wordpress Plugin Smart Product Review plugin for WordPress	Unrestricted Upload of File with Dangerous Type	The Wordpress Plugin Smart Product Review plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in all versions up to, and including, 1.0.4	https://www.exploit-db.com/exploits/50533 https://www.wordfence.com/threat-intel/vulnerabilities/id/1de9183c-95b9-4500-85e2-08dcee956360?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3785	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer Stack-based Buffer Overflow	D-Link DWR-M961 1.1.36	https://github.com/ZOKEYE/CVE/blob/main/D-link.md https://vuldb.com/?ctiid.305608 https://vuldb.com/?id.305608 https://vuldb.com/?submit.553547 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-3404	8,8	The Download Manager plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	The Download Manager plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the savePackage function in all versions up to, and including, 3.3.12	https://plugins.trac.wordpress.org/browser/download-manager/tags/3.3.12/src/Admin/Menu/Packages.php#L45 https://plugins.trac.wordpress.org/browser/download-manager/tags/3.3.12/src/Admin/Menu/Packages.php#L56 https://www.wordfence.com/threat-intel/vulnerabilities/id/21f8f5be-b513-4040-af39-c1a61d7e313f?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-3820	8,7	Tenda	Stack-based Buffer Overflow Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda W12 and i24 3.0.0.4(2887)/3.0.0.5(3644)	https://github.com/02Tn/vul/issues/4 https://vuldb.com/?ctiid.305726 https://vuldb.com/?id.305726 https://vuldb.com/?submit.555728 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-3854	8,0	H3C GR-3000AX	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	H3C GR-3000AX up to V100R006	https://github.com/CH13hh/tmp_store_cc/blob/main/H3C%20GR-3000AX/1.md https://vuldb.com/?ctiid.305778 https://vuldb.com/?id.305778 https://vuldb.com/?submit.556614 https://www.h3c.com/cn/Service/Document_Software/Software_Download/Consume_product/ https://zhiliao.h3c.com/theme/details/229784
https://nvd.nist.gov/vuln/detail/CVE-2025-1731	7,8	Zyxel USG FLEX H series uOS	Incorrect Permission Assignment for Critical Resource	uOS firmware versions from V1.20 through V1.31	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-incorrect-permission-assignment-and-improper-privilege-management-vulnerabilities-in-usg-flex-h-series-firewalls-04-22-2025
https://nvd.nist.gov/vuln/detail/CVE-2025-3847	7,3	markparticle WebServer	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	WebServer up to 1.0	https://magnificent-dill-351.notion.site/SQL-Injection-of-Login-in-WebServer-1-0-1d1c693918ed800b847bcc28bd691b7c https://vuldb.com/?ctiid.305775 https://vuldb.com/?id.305775 https://vuldb.com/?submit.556275

https://nvd.nist.gov/vuln/detail/CVE-2025-3809	7,2	The Debug Log Manager plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	The Debug Log Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the auto-refresh debug log in all versions up to, and including, 2.3.4	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3267252%40debug-log-manager&new=3267252%40debug-log-manager&sfp_email=&sfph_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/cbc3210d-224e-4ed2-ada7-dc17deb17584?source=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL

News

Σύντομη περιγραφή / Τίτλος	URL
“Microsoft’s Secure Future Initiative” Biggest Cybersecurity Project in Its History	https://cybersecuritynews.com/microsofts-secure-future-initiative-biggest-cybersecurity-project-in-its-history/
Digital Forensics In 2025: How CSOs Can Lead Effective Investigations	https://cybersecuritynews.com/digital-forensics-in-2025-how-csos-can-lead-effective-investigations/
Attack Via Infostealers Increased by 84% Via Phishing Emails Per Week	https://cybersecuritynews.com/attack-via-infostealers-increased/
Cybersecurity Metrics That Matter for Board-Level Reporting	https://cybersecuritynews.com/cybersecurity-metrics/
Business Continuity in a Digital World – CISO Perspectives	https://cybersecuritynews.com/business-continuity-in-a-digital-world/
The Role of Threat Intelligence in Proactive Defense	https://cybersecuritynews.com/role-of-threat-intelligence/
Ransomware Attack on Banks Costs an Average of $6.08 Million Along With Downtime & Reputation Loss	https://cybersecuritynews.com/ransomware-attack-on-banks-costs-an-average-of-6-08-million/
Cyber Security News Letter: Key Updates on Attacks, Vulnerabilities, & Data Breaches	https://cybersecuritynews.com/cyber-security-news-letter/
Fortinet Ends SSL-VPN Support From 7.6.3 Onwards!	https://cybersecuritynews.com/fortinet-ends-ssl-vpn-support/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
28-Year-Old Lost 2 Lakhs by Just Downloading Image in WhatsApp	https://cybersecuritynews.com/whatsapp-image-lost-2-lakhs/
U.S DOGE Allegedly Hacked – Fed Whistleblower Leaked Most Disturbing Documents	https://cybersecuritynews.com/doge-hacked/
17,000+ Fortinet Devices Compromised in Massive Hack via Symbolic Link Exploit	https://cybersecuritynews.com/fortinet-devices-compromised/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
WinZip MotW Bypass Vulnerability Let Hackers Execute Malicious Code Silently	https://cybersecuritynews.com/winzip-motw-bypass-vulnerability/
Windows Defender Policies Bypassed Using WinDbg Preview via Microsoft Store	https://cybersecuritynews.com/windows-defender-policies-bypassed/
CISA Warns of Multiple Apple 0-day Vulnerabilities Actively Exploited in Attacks	https://cybersecuritynews.com/apple-0-day-vulnerabilities-exploited/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
New Phishing Attack Appending Weaponized HTML Files Inside SVG Files	https://cybersecuritynews.com/new-phishing-attack-appending-weaponized-html-files/
Akira Ransomware Using Compromised Credentials and Public Tools in New Wave of Cyberattacks	https://cybersecuritynews.com/akira-ransomware-using-compromised-credentials-and-public-tools/
Hackers Weaponizing Certificates & Stolen Private Keys to Infiltrate Organizations	https://cybersecuritynews.com/hackers-weaponizing-certificates-stolen-private-keys/
RedGolf Hackers Expose Fortinet Exploits & Tools Used to Hack Organizations	https://cybersecuritynews.com/redgolf-exposes-fortinet-zero-day/
Hackers Leverage Zoom’s Remote Control Feature to Gain Users’ System Access	https://cybersecuritynews.com/zooms-remote-control-feature/
Speedify VPN macOS Vulnerability Let Attackers Escalate Privilege	https://cybersecuritynews.com/speedify-vpn-macos-vulnerability/
Beware! New Malware Mimics as Cisco Webex Attacks Users in-the-wild	https://cybersecuritynews.com/malware-mimics-cisco-webex/
Critical PyTorch Vulnerability Let Attackers Execute Remote Code	https://cybersecuritynews.com/critical-pytorch-vulnerability/
Critical ASUS Router Vulnerability Let Attackers Malicious Code Remotely	https://cybersecuritynews.com/critical-asus-router-vulnerability/
Hackers Bypassed Gmail’s Security Filters Bypassed for Sophisticated Phishing Attacks	https://cybersecuritynews.com/googles-oauth-system-flaws/
Linux Kernel Vulnerability Let Attackers Escalate Privilege – PoC Released	https://cybersecuritynews.com/linux-kernel-vulnerability-escalate-privilege/
Beware! Android Spyware ‘SpyMax’ Gain Total Control of Your Android Phone	https://cybersecuritynews.com/beware-android-spyware-spymax-gain-total-control/
6,000,000+ Installed Chrome Extensions Can Execute Remote Commands on User’s Browser	https://cybersecuritynews.com/malicious-chrome-extensions/
New XorDDoS Malware Allows Attackers to Create Sophisticated DDoS Bot Network	https://cybersecuritynews.com/new-xorddos-malware-allows-attackers/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Linux 6.15-rc3 Released With Fix for Multiple Kernel Fixes	**https://cybersecuritynews.com/linux-6-15-rc3-released/**

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Penetration Testing And Threat Hunting: Key Practices For Security Leaders	https://cybersecuritynews.com/penetration-testing-and-threat-hunting-key-practices-for-security-leaders/
Protecting Against Insider Threats – Strategies for CISOs	https://cybersecuritynews.com/iprotecting-against-insider-threats/
Zero Trust Architecture – A Step-by-Step Guide for CISOs	https://cybersecuritynews.com/zero-trust-architecture/
Building a Cyber Risk Appetite Statement for Your Organization	https://cybersecuritynews.com/cyber-risk-appetite-statement-2/
Automating Threat Intelligence Enrichment In Your SIEM With MISP	https://cybersecuritynews.com/automating-threat-intelligence-enrichment-in-your-siem-with-misp/
A Step-by-Step Guide To Implementing MITRE ATT&CK In Your SOC Workflows	https://cybersecuritynews.com/implementing-mitre-attck-in-soc/
Web Server Hardening Best Practices For Organizations Across Industries	https://cybersecuritynews.com/web-server-hardening-best-practices-for-organizations-across-industries/

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/