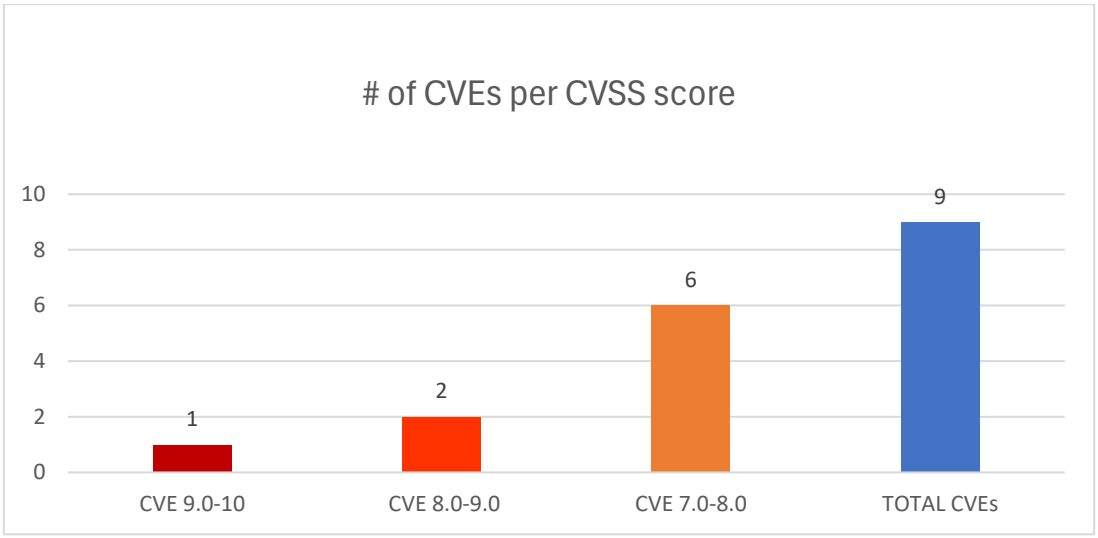
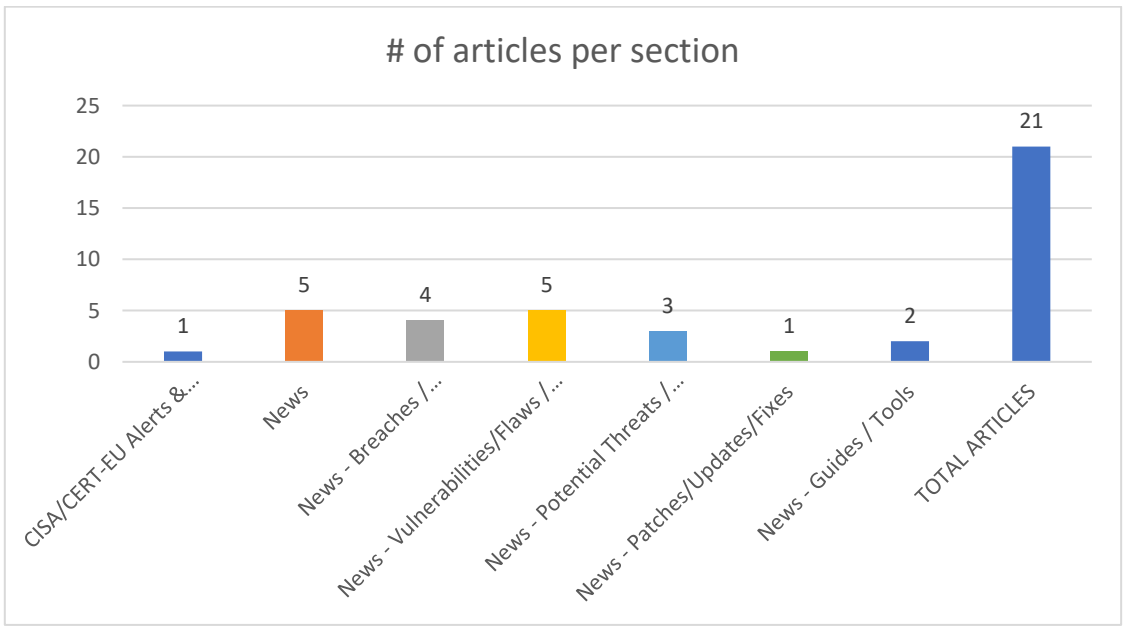

# Newsletter on system vulnerabilities and cybersecurity news.

## National Cyber Security Authority (NCSA)

**Date: 26/04/2025 - 29/04/2025**



# Contents

## Common Vulnerabilities and Exposures (CVEs)

| URL ευπάθειας (NIST NVD) | CVSSv3 | Προϊόν/Υπηρεσία | Τύπος Ευπάθειας | Συσκευές/Εκδόσεις που επηρεάζονται | URL προϊόντος/υπηρεσίας<br>URL οδηγιών αντιμετώπισης |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-3200 | **9,1** | the Com-Server and connected systems | Use of a Broken or Risky Cryptographic Algorithm | | https://certvde.com/en/advisories/VDE-2025-031/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-4007 | **8,8** | Tenda | Stack-based Buffer Overflow | Tenda W12 and i24 3.0.0.4(2887)/3.0.0.5(3644) | https://github.com/02Tn/vul/issues/5<br>https://vuldb.com/?ctiid.306343<br>https://vuldb.com/?id.306343<br>https://vuldb.com/?submit.558165<br>https://www.tenda.com.cn/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-3993 | **8,8** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory Buffer | N150RT 3.4.0-B20190525 | https://github.com/fizz-is-on-the-way/Iot_vuls/tree/main/N150RT/BufferOverflow_formWsc_1<br>https://vuldb.com/?ctiid.306329<br>https://vuldb.com/?id.306329<br>https://vuldb.com/?submit.557944<br>https://www.totolink.net/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-4014 | **7,3** | PHPGurukul Art Gallery Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | version 1.0 | https://github.com/ljfhhh/CVE/issues/2<br>https://phpgurukul.com/<br>https://vuldb.com/?ctiid.306367<br>https://vuldb.com/?id.306367<br>https://vuldb.com/?submit.558350 |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-3963 | **7,3** | Books-Management-System | Incorrect Authorization | version 1.0 | https://github.com/caigo8/CVE-md/blob/main/Blog-System/%E6%9C%AA%E6%8E%88%E6%9D%83%E8%AE%BF%E9%97%AE.md<br>https://vuldb.com/?ctiid.306299<br>https://vuldb.com/?id.306299<br>https://vuldb.com/?submit.557237 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-3998 | **7,3** | CodeAstro Membership Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | version 1.0 | https://codeastro.com/<br>https://github.com/lyg986443/cve/issues/4<br>https://vuldb.com/?ctiid.306334<br>https://vuldb.com/?id.306334<br>https://vuldb.com/?submit.557972 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-4023 | **7,3** | Placement Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | version 1.0 | https://github.com/xingyu-wu4678/cve/issues/1<br>https://itsourcecode.com/<br>https://vuldb.com/?ctiid.306377<br>https://vuldb.com/?id.306377<br>https://vuldb.com/?submit.558546 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-4026 | **7,3** | PHPGurukul Nipah Virus Testing Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | version 1.0 | https://github.com/changan520374/cve/issues/1<br>https://github.com/changan520374/cve/issues/1<br>https://phpgurukul.com/<br>https://vuldb.com/?ctiid.306389<br>https://vuldb.com/?id.306389<br>https://vuldb.com/?submit.558628 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-4031 | **7,3** | PHPGurukul Pre-School Enrollment System 1.0 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | version 1.0 | https://github.com/tailin1122/myCVE/issues/1<br>https://phpgurukul.com/<br>https://vuldb.com/?ctiid.306394<br>https://vuldb.com/?id.306394<br>https://vuldb.com/?submit.559221 |

## CISA/CERT-EU Alerts & Advisories

| Σύντομη περιγραφή / Τίτλος | Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες | URL |
|---|---|---|
| CISA Adds Three Known Exploited Vulnerabilities to Catalog | ▪ CVE-2025-1976 Broadcom Brocade Fabric OS Code Injection Vulnerability<br>▪ CVE-2025-42599 Qualitia Active! Mail Stack-Based Buffer Overflow Vulnerability<br>▪ CVE-2025-3928 Commvault Web Server Unspecified Vulnerability | https://www.cisa.gov/news-events/alerts/2025/04/28/cisa-adds-three-known-exploited-vulnerabilities-catalog |

## News

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Finding Child Abuse Sites on the Darkweb | https://infosecwriteups.com/finding-child-abuse-sites-on-the-darkweb-efc3a954caf6?source=collection_home |
| GoSearch: Open-source OSINT tool for uncovering digital footprints | https://www.helpnetsecurity.com/2025/04/28/gosearch-open-source-osint/ |
| ISACA Highlights Critical Lack of Quantum Threat Mitigation Strategies | https://www.infosecurity-magazine.com/news/isaca-lack-quantum-threat/ |
| CEO of cybersecurity firm charged with installing malware on hospital systems | https://securityaffairs.com/177020/cyber-crime/ceo-of-cybersecurity-firm-charged-with-installing-malware-on-hospital-systems.html |
| The Three Protocols That Could Bring Down The Internet (And Life as We Know It): DNS, PKI and BGP | https://medium.com/@billatnapier/the-three-protocols-that-could-bring-down-the-internet-and-life-as-we-know-it-dns-pki-and-bgp-e9b0c0b08df4 |

## Breaches / Compromised / Hacked

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| African multinational telco giant MTN Group disclosed a data breach | https://securityaffairs.com/177037/security/african-multinational-telco-giant-mtn-disclosed-a-data-breach.html |
| Hackers Exploit Critical Craft CMS Flaws; Hundreds of Servers Likely Compromised | https://thehackernews.com/2025/04/hackers-exploit-critical-craft-cms.html |
| JokerOTP Dismantled After 28,000 Phishing Attacks, 2 Arrested | https://hackread.com/jokerotp-dismantled-28000-phishing-attacks-2-arrested/ |
| VeriSource now says February data breach impacts 4 million people | https://www.bleepingcomputer.com/news/security/verisource-now-says-february-data-breach-impacts-4-million-people/ |

## Vulnerabilities / Flaws / Zero-day

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Critical SAP NetWeaver flaw exploited by suspected initial access broker (CVE-2025-31324) | https://www.helpnetsecurity.com/2025/04/28/sap-netweaver-cve-2025-31324-exploited/ |
| A large-scale phishing campaign targets WordPress WooCommerce users | https://securityaffairs.com/177115/hacking/a-large-scale-phishing-campaign-targets-wordpress-woocommerce-users.html |
| Kali Linux warns of update failures after losing repo signing key | https://www.bleepingcomputer.com/news/linux/kali-linux-warns-of-update-failures-after-losing-repo-signing-key/ |
| CISA Adds Actively Exploited Broadcom and Commvault Flaws to KEV Database | https://thehackernews.com/2025/04/cisa-adds-actively-exploited-broadcom.html |
| BreachForums Displays Message About Shutdown, Cites MyBB 0day Flaw | https://hackread.com/breachforums-displays-message-shutdown-mybb-0day-flaw/ |

## Patches / Updates / Fixes

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Microsoft fixes Outlook on the web search issues, failures | https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-outlook-on-the-web-search-issues-failures/ |

## Potential threats / Threat intelligence

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Ransomware attacks are getting smarter, harder to stop | https://www.helpnetsecurity.com/2025/04/28/companies-impacted-ransomware-attacks/ |
| PoC rootkit Curing evades traditional Linux detection systems | https://securityaffairs.com/177098/hacking/poc-rootkit-curing-evades-traditional-linux-detection-systems.html |
| CAPTCHA Chaos: From X Threads to Telegram | https://www.infostealers.com/article/captcha-chaos-from-x-threads-to-telegram/ |

## Guides / Tools

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Top 10 Best Cyber Attack Simulation Tools – 2025 | https://cybersecuritynews.com/cyber-attack-simulation-tools/ |
| Top Cybersecurity Tools of 2025 To Managing Remote Device Threats | https://cybersecuritynews.com/top-cybersecurity-tools-managing-remote-device-threats/ |

## 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/<br>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<br>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<br>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/ |