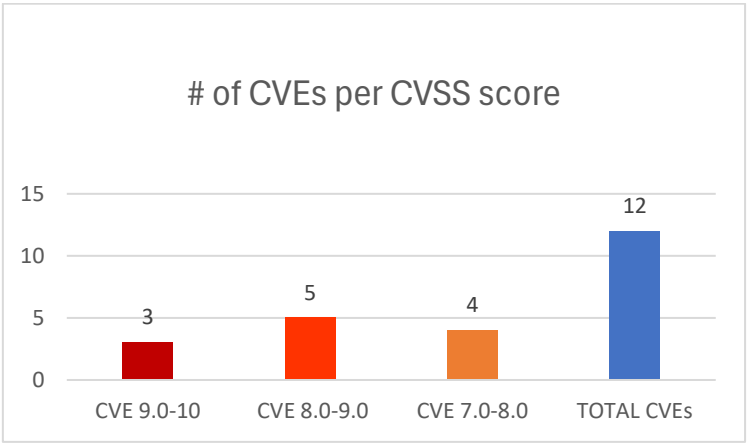
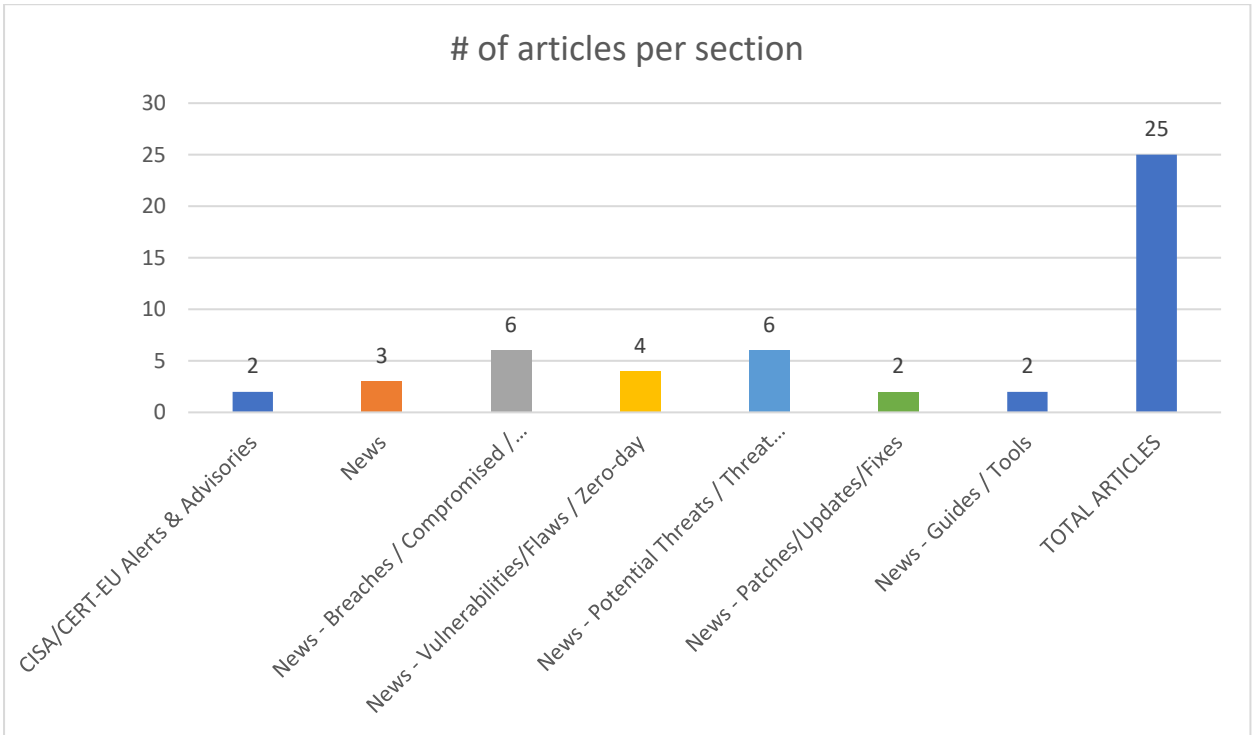

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

**Date: 05/07/2025 - 08/07/2025**



# 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-2025-41672 | 10,0 | WAGO GmbH & Co. KG | Insecure Default Initialization of Resource | 1.0.0 | https://cert.vde.com/en/advisories/VDE-2025-057<br>https://wago.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-057.json |
| https://nvd.nist.gov/vuln/detail/CVE-2025-3626 | 9,1 | OS Command | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | | https://certvde.com/en/advisories/VDE-2025-030 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-4779 | 9,1 | lunary-ai/lunary | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | versions prior to 1.9.24 | https://github.com/lunary-ai/lunary/commit/18750294a76ff6c0f3f1b6af4ac1a23399836b16<br>https://huntr.com/bounties/c603b64e-5171-4eed-8983-a7f656ce2c4d |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7077 | 8,8 | Shenzhen Libituo Technology | Improper Restriction of Operations within the Bounds of a Memory Buffer<br>Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | Shenzhen Libituo Technology LBT-T300-T310 up to 2.2.3.6 | https://github.com/FLY200503/IoT-vul/tree/master/LBT-T300<br>https://vuldb.com/?ctiid.314991<br>https://vuldb.com/?id.314991<br>https://vuldb.com/?submit.603012 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7094 | 8,8 | Belkin | Improper Restriction of Operations within the Bounds of a Memory Buffer<br>Stack-based Buffer Overflow | Belkin F9K1122 1.00.33 | https://github.com/wudipjq/my_vuln/blob/main/Belkin/vuln_14/14.md<br>https://github.com/wudipjq/my_vuln/blob/main/Belkin/vuln_14/14.md#poc<br>https://vuldb.com/?ctiid.315008<br>https://vuldb.com/?id.315008<br>https://vuldb.com/?submit.603711 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7118 | 8,8 | UTT | Improper Restriction of Operations within the Bounds of a Memory Buffer<br>Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | UTT HiPER 840G up to 3.1.1-190328 | https://github.com/d2pq/cve/blob/main/616/8.md<br>https://github.com/d2pq/cve/blob/main/616/8.md#poc<br>https://vuldb.com/?ctiid.315029<br>https://vuldb.com/?id.315029<br>https://vuldb.com/?submit.605875 |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-7097 | 8,1 | Comodo Internet Security | Improper Neutralization of Special Elements used in a Command ('Command Injection')<br>Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | Comodo Internet Security Premium 12.3.4.8162 | https://drive.google.com/file/d/1qnWarYsTSc5_sV6o8ULv0LBvGfKKXPxn/view?usp=sharing<br>https://vuldb.com/?ctiid.315011<br>https://vuldb.com/?id.315011<br>https://vuldb.com/?submit.603714 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-53536 | 8,1 | Roo Code | Files or Directories Accessible to External Parties | Prior to 3.22.6 | https://github.com/RooCodeInc/Roo-Code/commit/1be6fce1a6864ae63e8160b0666db2c647f2dbba<br>https://github.com/RooCodeInc/Roo-Code/commit/3993406ebdc0553a32ef391a799a4fb124930a1c<br>https://github.com/RooCodeInc/Roo-Code/security/advisories/GHSA-3765-5vjr-qjgm |
| https://nvd.nist.gov/vuln/detail/CVE-2025-6209 | 7,5 | llama/llama_index | Path Traversal: '\..\filename' | versions 0.12.27 through 0.12.40 | https://github.com/run-llama/llama_index/commit/cdeaab91a204d1c3527f177dac37390327aef274<br>https://huntr.com/bounties/e89d14f8-bfe8-4c9a-bb2a-656c01cc9a68<br>https://huntr.com/bounties/e89d14f8-bfe8-4c9a-bb2a-656c01cc9a68 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-6386 | 7,5 | The parisneo/lollms repository | Observable Discrepancy | lollms_authentication.py` file | https://github.com/parisneo/lollms/commit/f78437f7b5aa39a78c6201912faf4e0645a38c48<br>https://huntr.com/bounties/6da05485-d219-4f18-9ffc-991053524b67 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7128 | 7,3 | Campcodes Payroll Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 1.0 | https://github.com/wyl091256/CVE/issues/15<br>https://github.com/wyl091256/CVE/issues/15<br>https://vuldb.com/?ctiid.315040<br>https://vuldb.com/?id.315040<br>https://vuldb.com/?submit.605945<br>https://www.campcodes.com/ |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-7145 | 7,2 | ThreatSonar Anti-Ransomware developed by TeamT5 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | ThreatSonar Anti-Ransomware developed by TeamT5 | https://www.twcert.org.tw/en/cp-139-10232-f99c0-2.html<br>https://www.twcert.org.tw/tw/cp-132-10231-a15c8-1.html |

## CISA/CERT-EU Alerts & Advisories

| Σύντομη περιγραφή / Τίτλος | Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες | URL |
|---|---|---|
| CISA Adds Four Known Exploited Vulnerabilities to Catalog | ▪ CVE-2014-3931 Multi-Router Looking Glass (MRLG) Buffer Overflow Vulnerability<br>▪ CVE-2016-10033 PHPMailer Command Injection Vulnerability<br>▪ CVE-2019-5418 Rails Ruby on Rails Path Traversal Vulnerability<br>▪ CVE-2019-9621 Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery (SSRF) Vulnerability | https://www.cisa.gov/news-events/alerts/2025/07/07/cisa-adds-four-known-exploited-vulnerabilities-catalog |
| U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Chromium V8 vulnerability to its Known Exploited Vulnerabilities catalog. | ▪ CVE-2025-6554 | https://securityaffairs.com/179682/hacking/u-s-cisa-adds-google-chromium-v8-flaw-to-its-known-exploited-vulnerabilities-catalog.html |

## News

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| New Batavia spyware targets Russian industrial enterprises | https://securityaffairs.com/179699/uncategorized/new-batavia-spyware-targets-russian-industrial-enterprises.html |
| Iran-Aligned Hacking Group Targets Middle Eastern Governments | https://www.infosecurity-magazine.com/news/iran-hacking-group-targets-middle/ |
| TAG-140 Deploys DRAT V2 RAT, Targeting Indian Government, Defense, and Rail Sectors | https://thehackernews.com/2025/07/tag-140-deploys-drat-v2-rat-targeting.html |

## Breaches / Compromised / Hacked

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Telefónica Faces New Data Leak Allegations After Hacker Publishes Sample Files | https://dailysecurityreview.com/security-spotlight/telefonica-faces-new-data-leak-allegations-after-hacker-publishes-sample-files/ |
| BMW Financial Services Caught in Third-Party Data Breach Involving Texas Fintech Firm | https://dailysecurityreview.com/security-spotlight/bmw-financial-services-caught-in-third-party-data-breach-involving-texas-fintech-firm/ |
| SatanLock Ransomware Ends Operations, Says Stolen Data Will Be Leaked | https://hackread.com/satanlock-ransomware-ends-operations-stolen-data-leak/ |
| IT Giant Ingram Micro Reveals Ransomware Breach | https://www.infosecurity-magazine.com/news/it-giant-ingram-micro-reveals/ |
| Threat Actors Turning Job Offers Into Traps, Over $264 Million Lost in 2024 Alone | https://cybersecuritynews.com/threat-actors-turning-job-offers-into-traps/ |
| Chrome Store Features Extension Poisoned With Sophisticated Spyware | https://www.darkreading.com/endpoint-security/chrome-store-features-extension-poisoned-sophisticated-spyware |

## Vulnerabilities / Flaws / Zero-day

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Public exploits released for Citrix Bleed 2 NetScaler flaw, patch now | https://www.bleepingcomputer.com/news/security/public-exploits-released-for-citrixbleed-2-netscaler-flaw-patch-now/ |
| Comodo Internet Security 2025 Vulnerabilities Execute Remote Code With SYSTEM Privilege | https://cybersecuritynews.com/comodo-internet-security-2025-vulnerability/ |
| Linux Boot Vulnerability Allows Bypass of Secure Boot Protections on Modern Linux Systems | https://cybersecuritynews.com/linux-boot-vulnerability-allows-bypass-of-secure-boot-protections/ |
| Alert: Exposed JDWP Interfaces Lead to Crypto Mining, Hpingbot Targets SSH for DDoS | https://thehackernews.com/2025/07/alert-exposed-jdwp-interfaces-lead-to.html |

## Patches / Updates / Fixes

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Week in review: Sudo local privilege escalation flaws fixed, Google patches actively exploited Chrome | https://www.helpnetsecurity.com/2025/07/06/week-in-review-sudo-local-privilege-escalation-flaws-fixed-google-patches-actively-exploited-chrome/ |
| Microsoft to Remove PowerShell 2.0 from Windows 11 Due to Security Risks | https://cybersecuritynews.com/powershell-2-0-deprecation/ |

## Potential threats / Threat intelligence

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| BERT Ransomware Forcibly Shut Down ESXi Virtual Machines to Disrupt Recovery | https://cybersecuritynews.com/bert-ransomware-esxi-virtual-machines/ |
| Malware Surge Hits Android: Adware, Trojans and Crypto Theft Lead Q2 Threats | https://hackread.com/android-malware-adware-trojan-crypto-theft-q2-threats/ |
| Parrot OS 6.4 Released With Update For Popular Penetration Testing Tools | https://cybersecuritynews.com/parrot-os-6-4/ |
| Hackers abuse leaked Shellter red team tool to deploy infostealers | https://www.bleepingcomputer.com/news/security/hackers-abuse-leaked-shellter-red-team-tool-to-deploy-infostealers/ |
| RingReaper – New Linux EDR Evasion Tool Using io_uring Kernel Feature | https://cybersecuritynews.com/ringreaper-edr-evasion/ |
| NordDragonScan Attacking Windows Users to Steal Login Credentials | https://cybersecuritynews.com/norddragonscan-attacking-windows-users/ |

## 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.

[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/ |