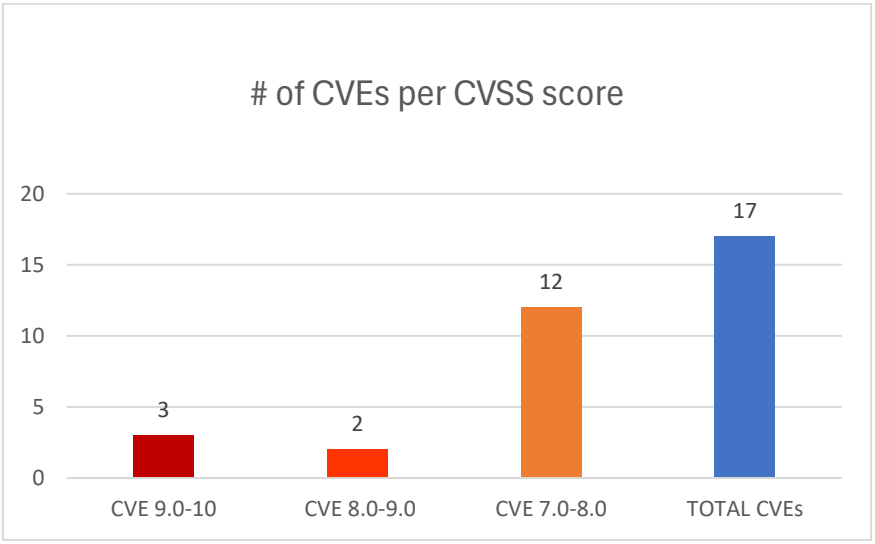
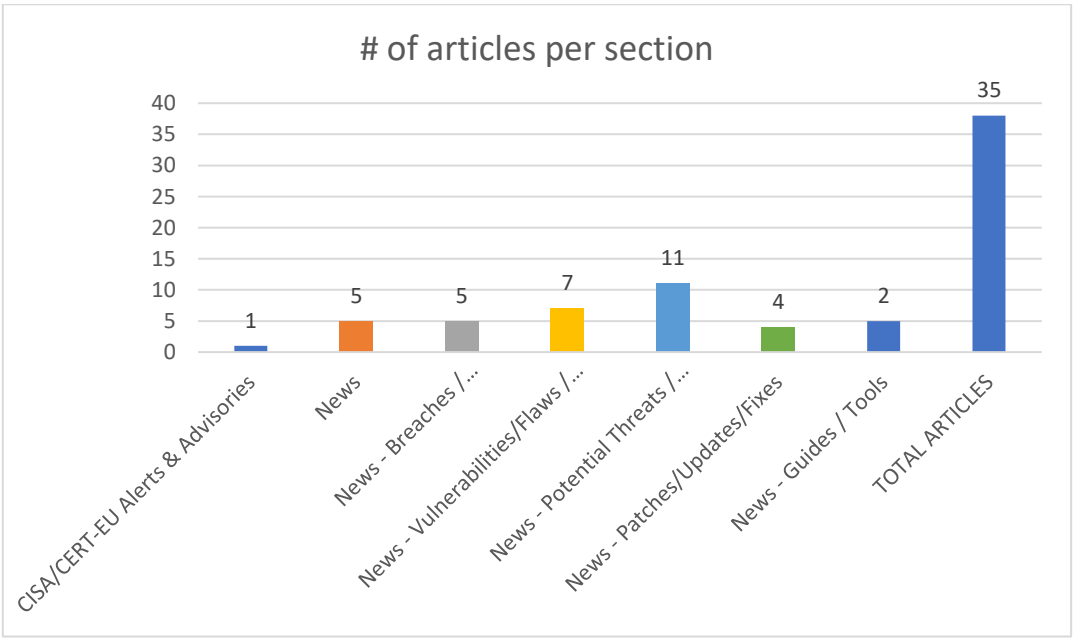
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 17/05/2025 - 20/05/2025





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-2025-47916	10,0	Invision Community	Improper Neutralization of Special Elements Used in a Template Engine	Invision Community 5.0.0 before 5.0.7	http://seclists.org/fulldisclosure/2025/May/4 https://invisioncommunity.com/release-notes-v5/507-r41/ https://karmainsecurity.com/KIS-2025-02 https://karmainsecurity.com/KIS-2025-02
https://debricked.com/vulnerability-database/vulnerability/CVE-2025-40906	9,8	BSON::XS	Use of Unmaintained Third Party Components	BSON::XS versions 0.8.4 and earlier for Perl	https://lists.debian.org/debian-lts-announce/2025/05/msg00012.html https://www.mongodb.com/community/forums/t/mongodb-perl-driver-end-of-life/7890
https://nvd.nist.gov/vuln/detail/CVE-2025-4802	9,8	GNU C Library	Untrusted Search Path	GNU C Library version 2.27 to 2.38	http://www.openwall.com/lists/oss-security/2025/05/16/7 http://www.openwall.com/lists/oss-security/2025/05/17/2 https://sourceware.org/bugzilla/show_bug.cgi?id=32976 https://sourceware.org/cgit/glibc/commit/?id=1e18586c5820e329f741d5c710275e165581380e
https://nvd.nist.gov/vuln/detail/CVE-2025-4733	8,8	TOTOLINK	Improper Restriction of Operations within the Bounds of a Memory Buffer	TOTOLINK A3002R and A3002RU 3.0.0-B20230809.1615	https://github.com/CH13hh/tmp_store_cc/blob/main/tt/ta/7.md https://vuldb.com/?ctiid.309035 https://vuldb.com/?id.309035 https://vuldb.com/?submit.570703 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-4809	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC7 15.03.06.44	https://lavender-bicycle-a5a.notion.site/Tenda-AC7-fromSafeSetMacFilter-1ed53a41781f80cbbf13c8d4cc405ed1?pvs=4 https://vuldb.com/?ctiid.309264 https://vuldb.com/?id.309264 https://vuldb.com/?submit.573642 https://www.tenda.com.cn/

https://nvd.nist.gov/vuln/detail/CVE-2024-53827	7,5	Ericsson	Improper Input Validation	Ericsson Packet Core Controller (PCC)	https://www.ericsson.com/en/about-us/security/psirt/CVE-2024-53827
https://nvd.nist.gov/vuln/detail/CVE-2025-1975	7,5	Ollama Server	Improper Validation of Array Index	Ollama server version 0.5.11	https://huntr.com/bounties/921ba5d4-f1d0-4c66-9764-4f72dffe7acd
https://nvd.nist.gov/vuln/detail/CVE-2025-47287	7,5	Tornado, Python web framework	Allocation of Resources Without Limits or Throttling	Tornado is a Python web framework and asynchronous networking library	https://github.com/tornadoweb/tornado/commit/b39b892bf78fe8fea01dd45199aa88307e7162f3 https://github.com/tornadoweb/tornado/security/advisories/GHSA-7cx3-6m66-7c5m
https://nvd.nist.gov/vuln/detail/CVE-2025-4749	7,5	D-Link	Improper Resource Shutdown or Release	D-Link DI-7003GV2 24.04.18D1 R(68125)	https://github.com/at0de/my_vulns/blob/main/Dlink/Di-7003GV2/backup.md https://vuldb.com/?ctiid.309052 https://vuldb.com/?id.309052 https://vuldb.com/?submit.571068 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-4755	7,3	D-Link	Improper Authentication	D-Link DI-7003GV2 24.04.18D1 R(68125)	https://github.com/at0de/my_vulns/blob/main/Dlink/Di-7003GV2/netconfig.md https://vuldb.com/?ctiid.309057 https://vuldb.com/?id.309057 https://vuldb.com/?submit.571073 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-4788	7,3	FreeFloat FTP Server	Improper Restriction of Operations within the Bounds of a Memory Buffer	FreeFloat FTP Server 1.0	https://fitoxs.com/exploit/exploit-cd619c9271a231511f4fa2de1cf569b7040376a5cfe23dc6060884c32638254e.txt https://fitoxs.com/exploit/exploit-cd619c9271a231511f4fa2de1cf569b7040376a5cfe23dc6060884c32638254e.txt https://vuldb.com/?ctiid.309097 https://vuldb.com/?id.309097 https://vuldb.com/?submit.572476

https://nvd.nist.gov/vuln/detail/CVE-2025-4792	7,3	FreeFloat FTP Server		FreeFloat FTP Server 1.0	https://fitoxs.com/exploit/exploit-fb7e880a8c21bdec1f4d3953a2c57bcc582b95ffc83513c7d709f45c15d60504.txt https://vuldb.com/?ctiid.309101 https://vuldb.com/?id.309101 https://vuldb.com/?submit.572481
https://nvd.nist.gov/vuln/detail/CVE-2025-4871	7,3	PCMan FTP Server	Improper Restriction of Operations within the Bounds of a Memory Buffer	PCMan FTP Server 2.0.7	https://github.com/Blu3B3ard/PoC-Pacman-FTP-Server-2.0.7/blob/main/exploit.txt https://vuldb.com/?ctiid.309413 https://vuldb.com/?id.309413 https://vuldb.com/?submit.575624
https://nvd.nist.gov/vuln/detail/CVE-2025-4882	7,3	Restaurant Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Restaurant Management System 1.0	https://github.com/Cherish-Ink/CVE/issues/2 https://github.com/Cherish-Ink/CVE/issues/2 https://itsourcecode.com/ https://vuldb.com/?ctiid.309435 https://vuldb.com/?id.309435 https://vuldb.com/?submit.576285
https://nvd.nist.gov/vuln/detail/CVE-2025-4880	7,3	PHPGurukul News Portal	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	PHPGurukul News Portal 4.1	https://github.com/Schatten-42/MyCVE/issues/8 https://github.com/Schatten-42/MyCVE/issues/8 https://phpgurukul.com/ https://vuldb.com/?ctiid.309433 https://vuldb.com/?id.309433 https://vuldb.com/?submit.576264
https://nvd.nist.gov/vuln/detail/CVE-2025-4875	7,3	Campcodes Online Shopping Portal	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Campcodes Online Shopping Portal 1.0	https://github.com/arpcyber040/CVE/issues/2 https://github.com/arpcyber040/CVE/issues/2 https://vuldb.com/?ctiid.309418 https://vuldb.com/?id.309418 https://vuldb.com/?submit.576265 https://www.campcodes.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-4872	7,3	FreeFloat FTP Server	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	FreeFloat FTP Server 1.0	https://github.com/Blu3B3ard/PoC-FreeFloat-FTP-Server-1.0/blob/main/exploit.txt https://github.com/Blu3B3ard/PoC-FreeFloat-FTP-Server-1.0/blob/main/exploit.txt https://vuldb.com/?ctiid.309414 https://vuldb.com/?id.309414 https://vuldb.com/?submit.575631

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Six Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-4427 Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability ▪ CVE-2025-4428 Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability ▪ CVE-2024-11182 MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability ▪ CVE-2025-27920 Srimax Output Messenger Directory Traversal Vulnerability ▪ CVE-2024-27443 Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability ▪ CVE-2023-38950 ZKTeco BioTime Path Traversal Vulnerability	https://www.cisa.gov/news-events/alerts/2025/05/19/cisa-adds-six-known-exploited-vulnerabilities-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
Printer Company Offered Malicious Drivers Infected With XRed Malware	https://cybersecuritynews.com/malicious-drivers-infected-with-xred-malware/
Malware Mastermind Andrei Tarasov Evades US Extradition Returns to Russia	https://cybersecuritynews.com/andrei-tarasov-evades-us-extradition/
Windows 10 KB5058379 Update Boots PCs into Windows Recovery	https://cybersecuritynews.com/windows-10-kb5058379-update-boots-pcs/
Researchers Emulated VanHelsing Ransomware Advanced Tactics & Tools Used	https://cybersecuritynews.com/researchers-emulated-vanhelsing-ransomware/
Proofpoint To Acquire Microsoft 365 Security Provider Hornetsecurity For $1 Billion	https://cybersecuritynews.com/proofpoint-acquire-hornetsecurity/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Windows 11, Red Hat Linux, & Oracle VirtualBox Hacked – Pwn2Own Day 1	https://cybersecuritynews.com/windows-11-red-hat-linux-oracle-virtualbox-hacked-pwn2own-day-1/
Millions of Records Exposed via SQL Injection in a Tamil Nadu Government Portal	https://infosecwriteups.com/millions-of-records-exposed-via-sql-injection-in-a-tamil-nadu-government-portal-0981d3827ed2?source=collection_home
SK Telecom Data Breach Exposes Nearly 27 Million SIM Records	https://dailysecurityreview.com/security-spotlight/sk-telecom-data-breach-exposes-nearly-27-million-sim-records/
Broadcom Employee Data Leaked After Supply Chain Breach at ADP Partner	https://dailysecurityreview.com/security-spotlight/broadcom-employee-data-leaked-after-supply-chain-breach-at-adp-partner/
UK Legal Aid Agency confirms applicant data stolen in data breach	https://www.bleepingcomputer.com/news/security/uk-legal-aid-agency-confirms-applicant-data-stolen-in-data-breach/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Critical WordPress Plugin Vulnerability Exposes 10K+ Sites to Cyber Attack	https://cybersecuritynews.com/critical-wordpress-plugin-vulnerability/
VMware ESXi, Firefox, Red Hat Linux & SharePoint 0-Day Vulnerabilities Exploited – Pwn2Own Day 2	https://cybersecuritynews.com/pwn2own-0-day-vulnerabilities/
RCE Vulnerability Found in RomethemeKit For Elementor Plugin	https://www.infosecurity-magazine.com/news/rce-vulnerability-in-romethemekit/
Over 40,000 iOS Apps Found Exploiting Private Entitlements, Zimperium	https://hackread.com/40000-ios-apps-found-exploiting-private-entitlements/
New Vulnerability Affects All Intel Processors From The Last 6 Years	https://cybersecuritynews.com/new-vulnerability-affects-all-intel-processors/
Ransomware Gangs Use Skitnet Malware for Stealthy Data Theft and Remote Access	https://thehackernews.com/2025/05/ransomware-gangs-use-skitnet-malware.html
CISA Warns of Google Chromium 0-Day Vulnerability Actively Exploited in the Wild – Patch Now!	https://cybersecuritynews.com/cisa-warns-of-google-chromium-vulnerability-actively-exploited-in-the-wild/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Jenkins Security Update Released With the Fixes for the Vulnerabilities that Exploit CI/CD Pipelines	https://cybersecuritynews.com/jenkins-security-update/
Week in review: Microsoft patches 5 actively exploited 0-days, recently fixed Chrome vulnerability exploited	https://www.helpnetsecurity.com/2025/05/18/week-in-review-microsoft-patches-5-actively-exploited-0-days-recently-fixed-chrome-vulnerability-exploited/
Firefox Patches 2 Zero-Days Exploited at Pwn2Own Berlin with $100K in Rewards	https://thehackernews.com/2025/05/firefox-patches-2-zero-days-exploited.html
Google to Release Android 16 with Advanced Device-level Security Setting Protection for 3 Billion Devices	https://cybersecuritynews.com/google-to-release-android-16-with-advanced-device-level-security-setting-protection/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Windows Remote Desktop Gateway UAF Vulnerability Allows Remote Code Execution	https://cybersecuritynews.com/windows-remote-desktop-gateway-uaf-vulnerability/
PupkinStealer Attacks Windows System to Steal Login Credentials & Desktop Files	https://cybersecuritynews.com/pupkinstealer-attacks-windows-system/
Sophisticated NPM Attack Exploits Google Calendar C2 For Sophisticated Communication	https://cybersecuritynews.com/sophisticated-npm-attack-exploits-google-calendar-c2/
New Ransomware Attack Mocking Elon Musk Supporters Using PowerShell to Deploy Payloads	https://cybersecuritynews.com/new-ransomware-attack-mocking-elon-musk-supporters-using-powershell/
New FrigidStealer Malware Attacking macOS Users to Steal Login Credentials	https://cybersecuritynews.com/new-frigidstealer-malware-attacking-macos-users/
APT Group 123 Actively Attacking Windows Systems to Deliver Malicious Payloads	https://cybersecuritynews.com/apt-group-123-actively-attacking-windows-systems/
Multiple Ivanti Endpoint Mobile Manager Vulnerabilities Allows Remote Code Execution	https://cybersecuritynews.com/ivanti-endpoint-mobile-manager-vulnerabilities/
Hackers Attacking Industrial Automation Systems With 11,600+ Malware Families	https://cybersecuritynews.com/hackers-attacking-with-11600-malware-families/
Hackers Actively Exploiting PowerShell to Evade Antivirus & EDR	https://cybersecuritynews.com/hackers-actively-exploiting-powershell/
SonicWall SMA1000 Vulnerability Let Attackers to Exploit Encoded URLs To Gain Internal Systems Access Remotely	https://cybersecuritynews.com/sonicwall-sma1000-vulnerability/
CTM360 maps out real-time phishing infrastructure targeting corporate banking worldwide	https://www.helpnetsecurity.com/2025/05/19/ctm360-cyberheist-phish-report/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
10 Best NGINX Monitoring Tools – 2025	https://cybersecuritynews.com/best-nginx-monitoring-tools/
Hands-on Malware Analysis Training to Boost Up SOC & MSSP Teams	https://cybersecuritynews.com/malware-analysis-training/

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/