NATIONAL CYBERSECURITY AUTHORITY GR

CVEs Alerts

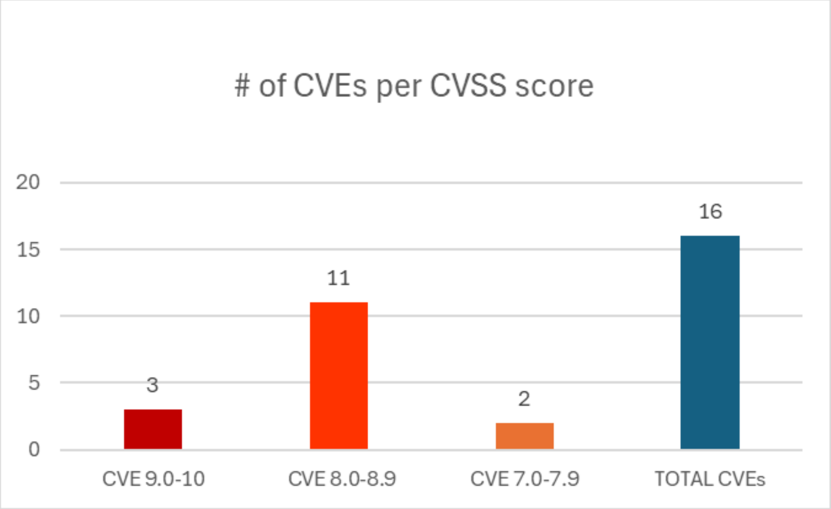
CVEs, CISA/CERT-EU Alerts Advisories & News

Newsletter on system vulnerabilities and cybersecurity news

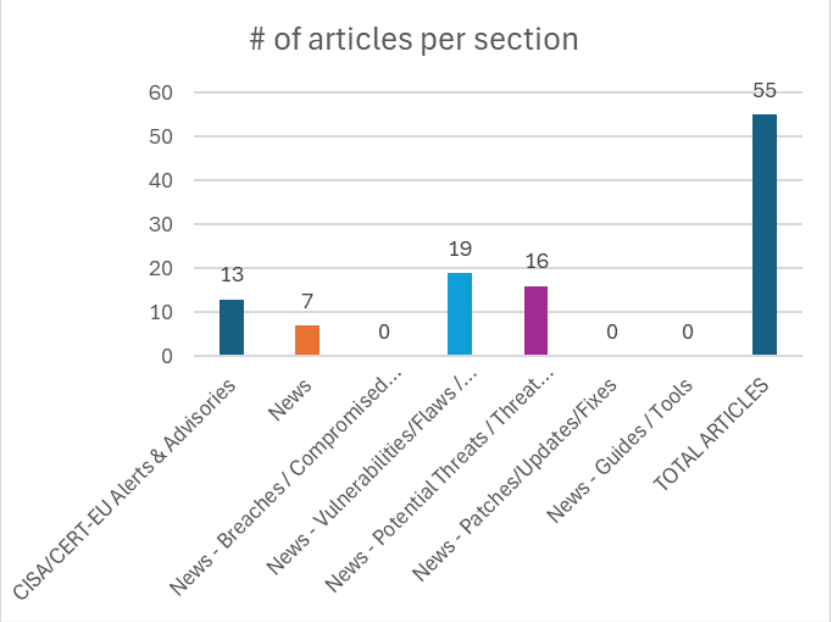
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 24/06/2025 - 27/06/2025



# 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-2025-20282	**10,0**	Cisco	Improper Privilege Management	API of Cisco ISE and Cisco ISE-PIC	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6
https://nvd.nist.gov/vuln/detail/CVE-2025-20281	**9,8**	Cisco	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	API of Cisco ISE and Cisco ISE-PIC	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6
https://nvd.nist.gov/vuln/detail/CVE-2025-36038	**9,0**	IBM WebSphere Application Server	Deserialization of Untrusted Data	IBM WebSphere Application Server 8.5 and 9.0	https://www.ibm.com/support/pages/node/7237967
https://nvd.nist.gov/vuln/detail/CVE-2025-36004	**8,8**	IBM	Uncontrolled Search Path Element	IBM i 7.2, 7.3, 7.4, and 7.5	https://www.ibm.com/support/pages/node/7237732
https://nvd.nist.gov/vuln/detail/CVE-2025-6565	**8,8**	Netgear	Stack-based Buffer Overflow Improper Restriction of Operations within the Bounds of a Memory Buffer	Netgear WNCE3001 1.0.0.50	https://github.com/xiaobor123/vul-finds/tree/main/vul-find-wnce3001-netgear https://github.com/xiaobor123/vul-finds/tree/main/vul-find-wnce3001-netgear#poc https://vuldb.com/?ctiid.313737 https://vuldb.com/?id.313737 https://vuldb.com/?submit.590030 https://www.netgear.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6568	**8,8**	TOTOLINK	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Improper Restriction of Operations within the Bounds of a Memory Buffer	TOTOLINK EX1200T 4.1.2cu.5232_B20210713	https://github.com/d2pq/cve/blob/main/616/23.md https://github.com/d2pq/cve/blob/main/616/23.md#poc https://vuldb.com/?ctiid.313740 https://vuldb.com/?id.313740 https://vuldb.com/?submit.601344 https://www.totolink.net/

https://nvd.nist.gov/vuln/detail/CVE-2025-6615	**8,8**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer Stack-based Buffer Overflow	D-Link DIR-619L 2.06B01	https://github.com/wudipjq/my_vuln/blob/main/D-Link6/vuln_76/76.md https://github.com/wudipjq/my_vuln/blob/main/D-Link6/vuln_76/76.md#poc https://vuldb.com/?ctiid.313833 https://vuldb.com/?id.313833 https://vuldb.com/?submit.602258 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6617	**8,8**	D-Link	Stack-based Buffer Overflow Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-619L 2.06B01	https://github.com/wudipjq/my_vuln/blob/main/D-Link6/vuln_78/78.md https://github.com/wudipjq/my_vuln/blob/main/D-Link6/vuln_78/78.md#poc https://vuldb.com/?ctiid.313835 https://vuldb.com/?id.313835 https://vuldb.com/?submit.602260 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6627	**8,8**	TOTOLINK	Improper Restriction of Operations within the Bounds of a Memory Buffer Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	TOTOLINK A702R 4.0.0-B20230721.1521	https://github.com/d2pq/cve/blob/main/616/24.md https://github.com/d2pq/cve/blob/main/616/24.md#poc https://vuldb.com/?ctiid.313852 https://vuldb.com/?id.313852 https://vuldb.com/?submit.602292 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-6733	**8,8**	UTT	mproper Restriction of Operations within the Bounds of a Memory Buffer 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/616/2.md https://github.com/d2pq/cve/blob/main/616/2.md#poc https://vuldb.com/?ctiid.314008 https://vuldb.com/?id.314008 https://vuldb.com/?submit.597678

https://nvd.nist.gov/vuln/detail/CVE-2025-6734	**8,8**	UTT	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Improper Restriction of Operations within the Bounds of a Memory Buffer	UTT HiPER 840G up to 3.1.1-190328	https://github.com/d2pq/cve/blob/main/616/3.md https://github.com/d2pq/cve/blob/main/616/3.md#poc https://vuldb.com/?ctiid.314009 https://vuldb.com/?id.314009 https://vuldb.com/?submit.597679
https://nvd.nist.gov/vuln/detail/CVE-2025-6751	**8,8**	Linksys	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Improper Restriction of Operations within the Bounds of a Memory Buffer	Linksys E8450 up to 1.2.00.360516	https://github.com/CH13hh/tmp_store_cc/blob/main/E8450/1.md https://github.com/CH13hh/tmp_store_cc/blob/main/E8450/1.md#poc https://vuldb.com/?ctiid.314049 https://vuldb.com/?id.314049 https://vuldb.com/?submit.598217 https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6752	**8,8**	Linksys	Stack-based Buffer Overflow Improper Restriction of Operations within the Bounds of a Memory Buffer	Linksys WRT1900ACS, EA7200, EA7450 and EA7500 up to 20250619	https://github.com/feiwuxingxie/cve/blob/main/linksys/vul01/1.md https://github.com/feiwuxingxie/cve/blob/main/linksys/vul01/1.md#poc https://vuldb.com/?ctiid.314050 https://vuldb.com/?id.314050 https://vuldb.com/?submit.600638 https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6032	**8,3**	Podman	Improper Certificate Validation		https://access.redhat.com/security/cve/CVE-2025-6032 https://bugzilla.redhat.com/show_bug.cgi?id=2372501
https://nvd.nist.gov/vuln/detail/CVE-2025-0966	**7,6**	IBM	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	IBM InfoSphere Information Server 11.7	https://www.ibm.com/support/pages/node/7236613

https://nvd.nist.gov/vuln/detail/CVE-2025-6614	**7,4**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer Stack-based Buffer Overflow	D-Link DIR-619L 2.06B01	https://github.com/wudipjq/my_vuln/blob/main/D-Link6/vuln_75/75.md https://github.com/wudipjq/my_vuln/blob/main/D-Link6/vuln_75/75.md#poc https://vuldb.com/?ctiid.313832 https://vuldb.com/?id.313832 https://vuldb.com/?submit.602257 https://www.dlink.com/

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
New Guidance Released for Reducing Memory-Related Vulnerabilities		https://www.cisa.gov/news-events/alerts/2025/06/24/new-guidance-released-reducing-memory-related-vulnerabilities
Kaleris Navis N4 Terminal Operating System		https://www.cisa.gov/news-events/ics-advisories/icsa-25-175-01
Delta Electronics CNCSoft		https://www.cisa.gov/news-events/ics-advisories/icsa-25-175-02
Schneider Electric Modicon Controllers		https://www.cisa.gov/news-events/ics-advisories/icsa-25-175-03
Schneider Electric EVLink WallBox		https://www.cisa.gov/news-events/ics-advisories/icsa-25-175-04
ControlID iDSecure On-Premises		https://www.cisa.gov/news-events/ics-advisories/icsa-25-175-05
Parsons AccuWeather Widget		https://www.cisa.gov/news-events/ics-advisories/icsa-25-175-06
MICROSENS NMP Web+		https://www.cisa.gov/news-events/ics-advisories/icsa-25-175-07
CISA Releases Eight Industrial Control Systems Advisories		https://www.cisa.gov/news-events/alerts/2025/06/24/cisa-releases-eight-industrial-control-systems-advisories
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2024-54085 AMI MegaRAC SPx Authentication Bypass by Spoofing Vulnerability ▪ CVE-2024-0769 D-Link DIR-859 Router Path Traversal Vulnerability ▪ CVE-2019-6693 Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability	https://www.cisa.gov/news-events/alerts/2025/06/25/cisa-adds-three-known-exploited-vulnerabilities-catalog
Mitsubishi Electric Air Conditioning Systems		https://www.cisa.gov/news-events/ics-advisories/icsa-25-177-01
TrendMakers Sight Bulb Pro		https://www.cisa.gov/news-events/ics-advisories/icsa-25-177-02
CISA Releases Two Industrial Control Systems Advisories	▪ ICSA-25-177-01 Mitsubishi Electric Air Conditioning Systems ▪ ICSA-25-177-02 TrendMakers Sight Bulb Pro	https://www.cisa.gov/news-events/alerts/2025/06/26/cisa-releases-two-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
Researchers Manipulated Windows Registry Using a C++ Program	https://cybersecuritynews.com/windows-registry-manipulated/
CISA Warns of FortiOS Hard-Coded Credentials Vulnerability Exploited in Attacks	https://cybersecuritynews.com/fortinet-fortios-hard-coded-credentials-vulnerability/
Five Hackers Behind Notorious Data Selling Platform BreachForums Arrested	https://cybersecuritynews.com/five-hackers-behind-breachforum/
INTERPOL Warns of Sharp Rise in Cyber Attacks Targeting Western and Eastern Africa	https://cybersecuritynews.com/interpol-warns-of-sharp-rise-in-cyber-attacks/
Windows 11 Update Configuration Hangs During Update Scanning	https://cybersecuritynews.com/windows-11-update-configuration/
New FileFix Attack Abuses Windows File Explorer to Execute Malicious Commands	https://cybersecuritynews.com/filefix-attack/
Facebook, Netflix, Microsoft Websites Hijacked to Insert Fake Phone Numbers	https://cybersecuritynews.com/search-parameter-injection-attack/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Mitsubishi Electric AC Systems Vulnerability Allows Remote Control Without User Interaction	https://cybersecuritynews.com/mitsubishi-electric-ac-systems-vulnerability/
HPE OneView for VMware vCenter Allows Escalation of Privileges	https://cybersecuritynews.com/hpe-oneview-for-vmware-vcenter/
Microsoft 365's Direct Send Exploited to Send Phishing Emails as Internal Users	https://cybersecuritynews.com/microsoft-365s-direct-send-exploited/
CISA Warns of D-Link Path Traversal Vulnerability Exploited in Attacks	https://cybersecuritynews.com/d-link-path-traversal-vulnerability-exploited/
Cisco Identity Services Engine RCE Vulnerability Allows Command Execution as Root User	https://cybersecuritynews.com/cisco-ise-rce-vulnerability/
IBM i Vulnerability Allows Let Attackers Escalate Privileges	https://cybersecuritynews.com/ibm-i-vulnerability-allows-let-attackers/
Firefox 140 Released With Fix for Code Execution Vulnerability – Update Now	https://cybersecuritynews.com/firefox-140-released/
Realtek Vulnerability Let Attackers Trigger DoS Attack via Bluetooth Secure Connections Pairing Process	https://cybersecuritynews.com/realtek-vulnerability-let-attackers-trigger-dos-attack/
Critical Kibana Vulnerabilities Allows Heap Corruption and Remote Code Execution	https://cybersecuritynews.com/kibana-vulnerabilities-allows-code-execution/
Chrome Security Update: Patch for 11 Vulnerabilities Enabling Malicious Code Execution	https://cybersecuritynews.com/chrome-security-update/
Linux CentOS Web Panel Vulnerability Let Attackers Execute Malicious Remote Code – PoC Released	https://cybersecuritynews.com/linux-centos-web-panel-vulnerability/
CISA Issued ICS Advisories Covering Current Vulnerabilities and Exploits	https://cybersecuritynews.com/cisa-issued-ics-advisories/
NVIDIA Megatron LM Vulnerability Let Attackers Inject Malicious Code	https://cybersecuritynews.com/nvidia-megatron-lm-vulnerability/
TeamViewer for Windows Vulnerability Let Attackers Delete Files Using SYSTEM Privileges	https://cybersecuritynews.com/teamviewer-windows-vulnerability/
OPPO Clone Phone Weak WiFi Hotspot Exposes Sensitive Data	https://cybersecuritynews.com/oppo-clone-phone-weak-wifi-hotspot/
Xiaomi's Interoperability App Vulnerability Let Hackers Gain Unauthorized Access to the Victim's Device	https://cybersecuritynews.com/xiaomis-interoperability-app-vulnerability/
WinRAR Directory Vulnerability Allows Arbitrary Code Execution Using a Malicious File	https://cybersecuritynews.com/winrar-vulnerability/
WhatsApp Banned on U.S. House Staffers Devices Due to Potential Security Risks	https://cybersecuritynews.com/whatsapp-banned/
Notepad++ Vulnerability Let Attacker Gain Complete System Control – PoC Released	https://cybersecuritynews.com/notepad-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
ClickFix Attack Emerges by Over 500% – Hackers Actively Using This Technique to Trick Users	https://cybersecuritynews.com/clickfix-attack-emerges-by-over-500/
APT-C-36 Hackers Attacking Government Institutions, Financial Organizations, and Critical Infrastructure	https://cybersecuritynews.com/apt-c-36-hackers-attacking-government-institutions/
Iranian APT35 Hackers Attacking High-Profile Cyber Security Experts & Professors from Israel	https://cybersecuritynews.com/iranian-apt35-hackers-attacking-high-profile-cyber-security-experts/
Iranian Spear-Phishing Attack Mimic Google, Outlook, and Yahoo Domains	https://cybersecuritynews.com/iranian-spear-phishing-attack/
Threat Actors Weaponize ChatGPT, Cisco AnyConnect, Google Meet, and Teams to Attacks SMB's	https://cybersecuritynews.com/threat-actors-weaponize-chatgpt-cisco-anyconnect-google-meet-and-teams/
Cybercriminals Abuse LLM Models to Aid in Their Criminal Hacking Activities	https://cybersecuritynews.com/cybercriminals-abuse-llm-models/
Chinese Hackers Deploying Pubload Malware by Weaponizing Tibetan Community Lures & Filenames	https://cybersecuritynews.com/chinese-hackers-deploying-pubload-malware/
TeamFiltration Pentesting Tool Weaponized to Hijack Microsoft Teams, Outlook, and Other Accounts	https://cybersecuritynews.com/hackers-leverage-teamfiltration-pentesting-framework/
New Malware Spotted in The Wild Using Prompt Injection to Manipulate AI Models Processing Sample	https://cybersecuritynews.com/new-malware-spotted-in-the-wild-using-prompt-injection/
Beware of Weaponized Wedding Invite Scams That Deploys SpyMax RAT on Android Devices	https://cybersecuritynews.com/beware-of-weaponized-wedding-invite-scams/
Multiple Brother Devices Vulnerabilities Open Devices for Hacking	https://cybersecuritynews.com/multiple-brother-devices-vulnerabilities/
NetNerve – AI Powered PCAP Analysis to Detect Anomalies & Potential Threats	https://cybersecuritynews.com/netnerve-pcap-analysis/
CISA Releases Guide to Reduce Memory Safety Vulnerabilities in Modern Software Development	https://cybersecuritynews.com/cisa-releases-guide-to-reduce-memory-safety-vulnerabilities/
Akamai Shares New Techniques for Defenders to Shutdown Cryptominer Attacks	https://cybersecuritynews.com/new-techniques-for-defenders-to-shutdown-cryptominer-attacks/
APT Hackers Abuse Microsoft ClickOnce to Execute Malware as Trusted Host	https://cybersecuritynews.com/apt-hackers-abuse-microsoft-clickonce/
Pro-Iranian Hacktivists Targeting US Networks Department of Homeland Security Warns	https://cybersecuritynews.com/pro-iranian-hacktivists-targeting-us-networks/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL

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/