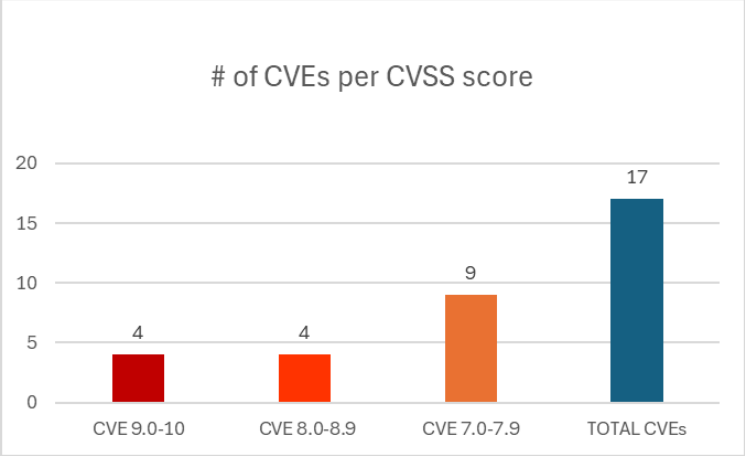
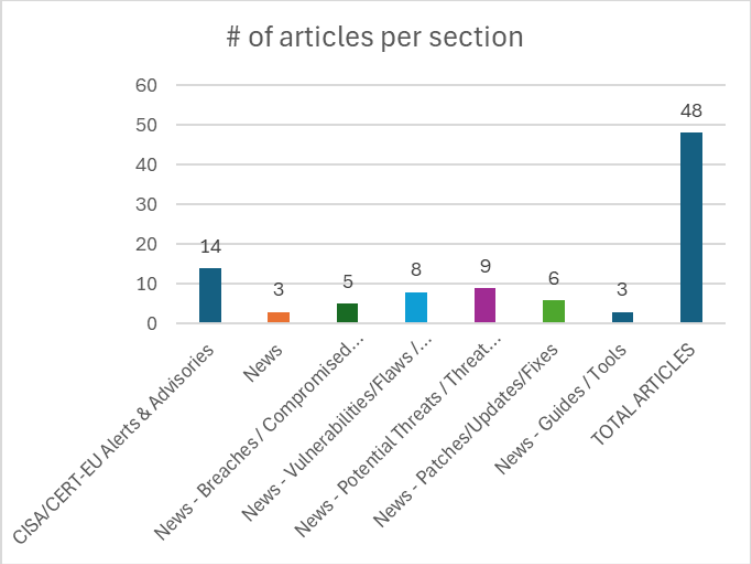
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 08/07/2025 - 11/07/2025





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-2025-4828	9,8	The Support Board plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 3.8.0	https://codecanyon.net/item/support-board-help-desk-and-chat/20359943 https://www.wordfence.com/threat-intel/vulnerabilities/id/33989611-8640-4c33-a34e-14f10cd7286d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-49533	9,8	Adobe Experience Manager (MS)	Deserialization of Untrusted Data	versions 6.5.23.0	https://helpx.adobe.com/security/products/aem-forms/apsb25-67.html
https://nvd.nist.gov/vuln/detail/CVE-2025-27203	9,6	Adobe Connect	Deserialization of Untrusted Data	versions 24.0	https://helpx.adobe.com/security/products/connect/apsb25-61.html
https://nvd.nist.gov/vuln/detail/CVE-2025-49535	9,3	ColdFusion	Improper Restriction of XML External Entity Reference	versions 2025.2, 2023.14, 2021.20	https://helpx.adobe.com/security/products/coldfusion/apsb25-69.html
https://nvd.nist.gov/vuln/detail/CVE-2025-7194	8,8	D-Link DI-500WF	Stack-based Buffer Overflow	17.04.10A1T	https://github.com/BigMancer/CVE/issues/1 https://vuldb.com/?ctiid.315133 https://vuldb.com/?id.315133 https://vuldb.com/?submit.607311 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-7422	8,8	Tenda	Stack-based Buffer Overflow mproper Restriction of Operations within the Bounds of a Memory Buffer	Tenda O3V2 1.0.0.12(3880)	https://github.com/wudipjq/my_vuln/blob/main/Tenda3/vuln_55/55.md https://github.com/wudipjq/my_vuln/blob/main/Tenda3/vuln_55/55.md#poc https://vuldb.com/?ctiid.315882 https://vuldb.com/?id.315882 https://vuldb.com/?submit.608868 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-7423	8,8	Tenda	Stack-based Buffer Overflow Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda O3V2 1.0.0.12(3880)	https://github.com/wudipjq/my_vuln/blob/main/Tenda3/vuln_56/56.md https://github.com/wudipjq/my_vuln/blob/main/Tenda3/vuln_56/56.md#poc https://vuldb.com/?ctiid.315883 https://vuldb.com/?id.315883 https://vuldb.com/?submit.608869 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-7434	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer Stack-based Buffer Overflow	Tenda FH451 up to 1.0.0.9	https://github.com/zezhifu1/cve_report/blob/main/FH451/fromAddressNat.md https://github.com/zezhifu1/cve_report/blob/main/FH451/fromAddressNat.md#payload https://vuldb.com/?ctiid.316004 https://vuldb.com/?id.316004 https://vuldb.com/?submit.609058 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-43582	7,8	Substance3D - Viewer	Heap-based Buffer Overflow	versions 0.22	https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-54.html
https://nvd.nist.gov/vuln/detail/CVE-2025-43591	7,8	InDesign Desktop	Heap-based Buffer Overflow	versions 19.5.3	https://helpx.adobe.com/security/products/indesign/apsb25-60.html

https://nvd.nist.gov/vuln/detail/CVE-2025-47099	7,8	InCopy	Heap-based Buffer Overflow	versions 20.3, 19.5.3	https://helpx.adobe.com/security/products/incopy/apsb25-59.html
https://nvd.nist.gov/vuln/detail/CVE-2025-47121	7,8	Adobe Framemaker	Access of Uninitialized Pointer	versions 2020.8, 2022.6	https://helpx.adobe.com/security/products/framemaker/apsb25-66.html
https://nvd.nist.gov/vuln/detail/CVE-2025-49526	7,8	Illustrator	Out-of-bounds Write	versions 28.7.6, 29.5.1	https://helpx.adobe.com/security/products/illustrator/apsb25-65.html
https://nvd.nist.gov/vuln/detail/CVE-2025-5040	7,8	Autodesk	Heap-based Buffer Overflow	Autodesk Revit	https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0012
https://nvd.nist.gov/vuln/detail/CVE-2025-7198	7,3	Jonnys Liquor	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0.	https://code-projects.org/ https://github.com/18889016001/cve/issues/2 https://vuldb.com/?ctiid.315136 https://vuldb.com/?id.315136 https://vuldb.com/?submit.607820
https://nvd.nist.gov/vuln/detail/CVE-2025-7199	7,3	Library System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/Gemileo/CVE/issues/2 https://vuldb.com/?ctiid.315137 https://vuldb.com/?id.315137 https://vuldb.com/?submit.607470
https://nvd.nist.gov/vuln/detail/CVE-2025-7211	7,3	LifeStyle Store	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/18889016001/cve/issues/4 https://vuldb.com/?ctiid.315160 https://vuldb.com/?id.315160 https://vuldb.com/?submit.607821

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog		https://www.cisa.gov/news-events/alerts/2025/07/10/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Thirteen Industrial Control Systems Advisories	▪ ICSA-25-191-01 Siemens SINEC NMS ▪ ICSA-25-191-02 Siemens Solid Edge ▪ ICSA-25-191-03 Siemens TIA Administrator ▪ ICSA-25-191-04 Siemens SIMATIC CN 4100 ▪ ICSA-25-191-05 Siemens TIA Project-Server and TIA Portal ▪ ICSA-25-191-06 Siemens SIPROTEC 5 ▪ ICSA-25-191-07 Delta Electronics DTM Soft ▪ ICSA-25-191-08 Advantech iView ▪ ICSA-25-191-09 KUNBUS RevPi Webstatus ▪ ICSA-25-191-10 End-of-Train and Head-of-Train Remote Linking Protocol ▪ ICSA-25-121-01 KUNBUS GmbH Revolution Pi (Update A) ▪ ICSA-25-135-19 ECOVACS DEEBOT Vacuum and Base Station (Update A) ▪ ICSA-24-263-02 IDEC Products (Update A)	https://www.cisa.gov/news-events/alerts/2025/07/10/cisa-releases-thirteen-industrial-control-systems-advisories
End-of-Train and Head-of-Train Remote Linking Protocol		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-10
KUNBUS RevPi Webstatus		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-09
Advantech iView		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-08
Delta Electronics DTM Soft		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-07
Siemens SIPROTEC 5		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-06
Siemens TIA Project-Server and TIA Portal		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-05
Siemens SIMATIC CN 4100		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-04
Siemens TIA Administrator		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-03
Siemens Solid Edge		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-02
Siemens SINEC NMS		https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-01
CISA Releases One Industrial Control Systems Advisory		https://www.cisa.gov/news-events/alerts/2025/07/08/cisa-releases-one-industrial-control-systems-advisory
Emerson ValveLink Products		https://www.cisa.gov/news-events/ics-advisories/icsa-25-189-01

News

Σύντομη περιγραφή / Τίτλος	URL
Iranian group Pay2Key.I2P ramps Up ransomware attacks against Israel and US with incentives for affiliates	https://securityaffairs.com/179754/malware/iranian-group-pay2key-i2p-ramps-up-ransomware-attacks-against-israel-and-us-with-incentives-for-affiliates.html
Microsoft Authenticator on iOS moves backups fully to iCloud	https://www.bleepingcomputer.com/news/microsoft/microsoft-authenticator-on-ios-moves-backups-fully-to-icloud/
Windows 11's New Black Screen of Death is Rolling Out for Users	https://cybersecuritynews.com/windows-11-black-screen-of-death/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Server with Rockerbox Tax Firm Data Exposed 286GB of Records	https://hackread.com/rockerbox-server-tax-firm-exposed-sensitive-records/
Bitcoin Depot Notifies Over 26,000 Customers of Year-Old Data Breach Involving Driver's License Information	https://dailysecurityreview.com/security-spotlight/bitcoin-depot-notifies-over-26000-customers-of-year-old-data-breach-involving-drivers-license-information/
McDonald's AI Hiring Bot With Password '123456' Leaks Millions of Job-Seekers Data	https://cybersecuritynews.com/mcdonalds-ai-hiring-bot-leaks/
Microsoft SQL Server 0-Day Vulnerability Exposes Sensitive Data Over Network	https://cybersecuritynews.com/microsoft-sql-server-0-day-vulnerability/
Nippon Steel Solutions suffered a data breach following a zero-day attack	https://securityaffairs.com/179766/data-breach/nippon-steel-solutions-data-breach.html?&web_view=true

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
New ServiceNow flaw lets attackers enumerate restricted data	https://www.bleepingcomputer.com/news/security/new-servicenow-flaw-lets-attackers-enumerate-restricted-data/
Ruckus Networks leaves severe flaws unpatched in management devices	https://www.bleepingcomputer.com/news/security/ruckus-networks-leaves-severe-flaws-unpatched-in-management-devices/
New Android TapTrap Attack Let Malicious Apps Bypass Permission and Carry out Destructive Actions	https://cybersecuritynews.com/android-taptrap-attack/
Multiple Apache Tomcat Vulnerabilities Let Attackers Trigger DoS Attacks	https://cybersecuritynews.com/apache-tomcat-dos-vulnerabilities/
Citrix Windows Virtual Delivery Agent Vulnerability Let Attackers Gain SYSTEM Privileges	https://cybersecuritynews.com/citrix-windows-virtual-delivery-agent-vulnerability/
Microsoft Remote Desktop Client Vulnerability Let Attackers Execute Remote Code	https://cybersecuritynews.com/microsoft-remote-desktop-client-vulnerability/
FortiWeb SQL Injection Vulnerability Allows Attacker to Execute Malicious SQL Code	https://cybersecuritynews.com/fortiweb-sql-injection-vulnerability/
Laravel APP_KEY Vulnerability Allows Remote Code Execution – Hundreds of Apps Affected	https://cybersecuritynews.com/laravel-app_key-rce-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Microsoft fixes critical wormable Windows flaw (CVE-2025-47981)	https://www.helpnetsecurity.com/2025/07/09/microsoft-fixes-critical-wormable-windows-flaw-cve-2025-47981/
Microsoft Patches Wormable RCE Vulnerability in Windows Client and Server	https://cybersecuritynews.com/microsoft-patches-wormable-rce-vulnerability/
Splunk Address Third-Party Packages Vulnerabilities in SOAR Versions – Update Now	https://cybersecuritynews.com/splunk-third-party-packages-soar-versions/
Ivanti, Fortinet, Splunk Release Security Updates	https://www.securityweek.com/ivanti-fortinet-splunk-release-security-updates/
Microsoft Patches 130 Vulnerabilities, Including Critical Flaws in SPNEGO and SQL Server	https://thehackernews.com/2025/07/microsoft-patches-130-vulnerabilities.html
Ingram Micro starts restoring systems after ransomware attack	https://www.bleepingcomputer.com/news/security/ingram-micro-starts-restoring-systems-after-ransomware-attack/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Hackers weaponize Shellter red teaming tool to spread infostealers	https://securityaffairs.com/179745/malware/hackers-weaponize-shellter-red-teaming-tool-to-spread-infostealers.html
Open source has a malware problem, and it's getting worse	https://www.helpnetsecurity.com/2025/07/10/open-source-malware-trends-2025/
Top 5 Remote-Access And RMM Tools Most Abused By Threat Actors	https://cybersecuritynews.com/top-5-remote-access-and-rmm-tools-most-abused-by-threat-actors/
VS Code Extension Weaponized With Two Lines of Code Leads to Supply Chain Attack	https://cybersecuritynews.com/vs-code-extension-weaponized/
New AI Malware PoC Reliably Evades Microsoft Defender	https://www.darkreading.com/endpoint-security/ai-malware-poc-evades-microsoft-defender
Windows BitLocker Bypass Vulnerability Let Attackers Bypass Security Feature	https://cybersecuritynews.com/windows-bitlocker-bypass-vulnerability/
SparkKitty Malware Attacking iOS and Android Device Users to Steal Photos From Gallery	https://cybersecuritynews.com/sparkkitty-attacking-ios-and-android-users/
Critical WordPress Plugin Vulnerability Exposes 200k Websites to Site Takeover Attack	https://cybersecuritynews.com/critical-wordpress-plugin-vulnerability-2/
New ZuRu Malware Variant Attacking macOS Users Via Weaponized Termius App	https://cybersecuritynews.com/new-zuru-malware-variant-attacking-macos-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/
Top 11 Best SysAdmin Tools in 2025	https://cybersecuritynews.com/sysadmin-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/ 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/