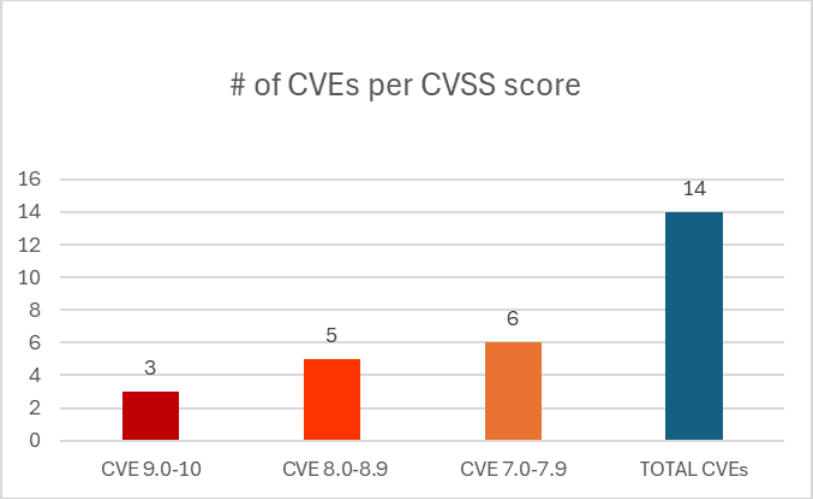
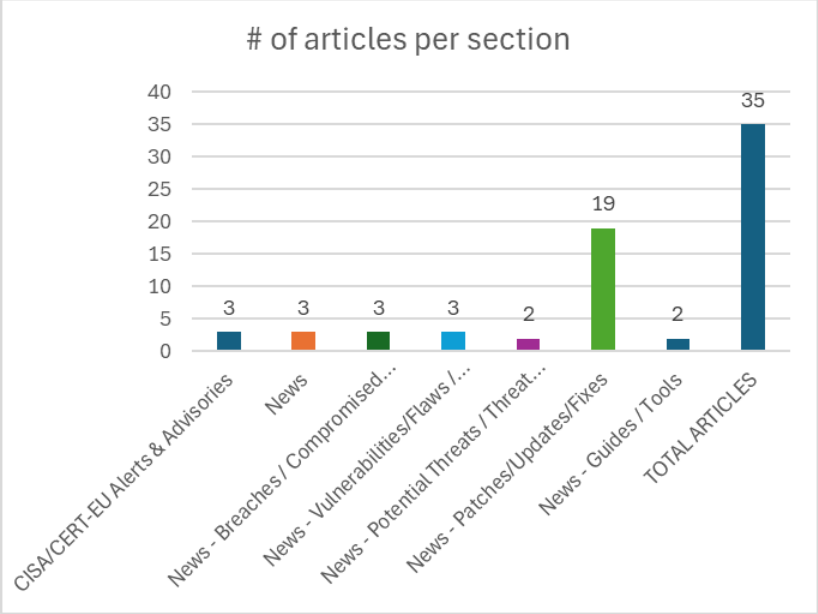
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 09/05/2025 - 13/05/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSS v3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-3605	9,8	The Frontend Login and Registration Blocks plugin for WordPress	Authorization Bypass Through User-Controlled Key	all versions up to, and including, 1.0.7	https://plugins.trac.wordpress.org/browser/frontend-login-and-registration-blocks/trunk/inc/class-flr-blocks-user-settings.php#L59 https://www.wordfence.com/threat-intel/vulnerabilities/id/0c11668c-6dc3-4539-b2be-bf6528bed73e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3811	9,8	WPBookit plugin for WordPress	Authorization Bypass Through User-Controlled Key	all versions up to, and including, 1.0.2	https://plugins.trac.wordpress.org/changeset/3278939/wpbookit/trunk/core/admin/classes/controllers/class.wpb-customer-controller.php https://www.wordfence.com/threat-intel/vulnerabilities/id/a61cce43-0df7-4ca9-8897-24c7d131b505?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-4556	9,3	GPM from WormHole	Unverified Password Change	The GPM from WormHole Tech	https://www.twcert.org.tw/en/cp-139-10115-f5f14-2.html https://www.twcert.org.tw/tw/cp-132-10114-10b4b-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-2158	8,8	The WordPress Review Plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 5.3.5 via the Post custom fields	https://plugins.trac.wordpress.org/browser/wp-review/tags/5.3.5/includes/functions.php https://plugins.trac.wordpress.org/browser/wp-review/tags/5.3.5/includes/shortcodes.php https://www.wordfence.com/threat-intel/vulnerabilities/id/a058e6bf-109f-4985-8aad-08858553c4c3?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-3455	**8,8**	1 Click WordPress Migration Plugin	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 2.2	https://plugins.trac.wordpress.org/browser/1-click-migration/trunk/inc/backup/class-ocm-backup.php#L403 https://www.wordfence.com/threat-intel/vulnerabilities/id/e982ae88-cfd0-46b9-ad64-00e398d307d6?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-4452	**8,8**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	D-Link DIR-619L 2.04B04	https://github.com/jylsec/vuldb/blob/main/D-Link/dlink_dir619l/Buffer_overflow-formSetWizard2-curTime/README.md https://vuldb.com/?ctiid.308066 https://vuldb.com/?id.308066 https://vuldb.com/?submit.560795 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-4462	**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 N150RT 3.4.0-B20190525	https://github.com/fizz-is-on-the-way/Iot_vuls/tree/main/N150RT/BufferOverflow_formWsc_2 https://vuldb.com/?ctiid.308081 https://vuldb.com/?id.308081 https://vuldb.com/?submit.565958 https://www.totolink.net/

https://nvd.nist.gov/vuln/detail/CVE-2025-4496	**8,8**	TOTOLINK T10	Improper Restriction of Operations within the Bounds of a Memory Buffer, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	A3100R, A950RG, A800R, N600R, A3000RU and A810R 4.1.8cu.5241_B20210927	https://github.com/CH13hh/tmp_store_cc/blob/main/tt/ta/1.md https://vuldb.com/?ctiid.308212 https://vuldb.com/?id.308212 https://vuldb.com/?submit.567081 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-1137	**7,5**	IBM Storage Scale	Improper Neutralization of Special Elements used in a Command ('Command Injection')	IBM Storage Scale 5.2.2.0 and 5.2.2.1	https://www.ibm.com/support/pages/node/7233085
https://nvd.nist.gov/vuln/detail/CVE-2025-3496	**7,5**	Bluetooth or RS-232 interface	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Bluetooth or RS-232 interface	https://cert.vde.com/en/advisories/VDE-2025-026
https://nvd.nist.gov/vuln/detail/CVE-2025-3632	**7,5**	IBM 4769	Memory Allocation with Excessive Size Value	IBM 4769 Developers Toolkit 7.0.0 through 7.5.52	https://www.ibm.com/support/pages/node/7233139

https://nvd.nist.gov/vuln/detail/CVE-2025-4494	**7,3**	JAdmin-JAVA	Improper Authentica-tion	JAdmin 1.0	https://github.com/JAdmin-JAVA/JAdmin/issues/1 https://github.com/JAdmin-JAVA/JAdmin/issues/1#issue-3012501470 https://vuldb.com/?ctiid.308208 https://vuldb.com/?id.308208 https://vuldb.com/?submit.566984
https://nvd.nist.gov/vuln/detail/CVE-2025-4540	**7,3**	MTSoftware C-Lodop	Unquoted Search Path or Element, Untrusted Search Path	MTSoftware C-Lodop 6.6.1.1	https://mega.nz/folder/A5lQQKpL#AF3WPzST3X1Ot6B6fs3bow https://vuldb.com/?ctiid.308285 https://vuldb.com/?id.308285 https://vuldb.com/?submit.566789
https://nvd.nist.gov/vuln/detail/CVE-2025-4525	**7,0**	Discord	Uncon-trolled Search Path Element, Untrusted Search Path	1.0.9188 on Windows	https://gist.github.com/shellkraft/ac4be6a3953e2889a7bf54aea2db88c2 https://vuldb.com/?ctiid.308270 https://vuldb.com/?id.308270 https://vuldb.com/?submit.562788

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Five Industrial Control Systems Advisories	▪ ICSA-25-128-01 Horner Automation Cscape ▪ ICSA-25-128-02 Hitachi Energy RTU500 series ▪ ICSA-25-128-03 Mitsubishi Electric CC-Link IE TSN ▪ ICSA-25-093-01 Hitachi Energy RTU500 Series (Update A) ▪ ICSMA-25-128-01 Pixmeo OsiriX MD	https://www.cisa.gov/news-events/alerts/2025/05/08/cisa-releases-five-industrial-control-systems-advisories
Update to How CISA Shares Cyber-Related Alerts and Notifications		https://www.cisa.gov/news-events/alerts/2025/05/12/update-how-cisa-shares-cyber-related-alerts-and-notifications
Vulnerability Summary for the Week of May 5, 2025		https://www.cisa.gov/news-events/bulletins/sb25-132

News

Σύντομη περιγραφή / Τίτλος	URL
FBI Warns of Hackers Compromising End-of-Life Routers to Hide Their Activity	https://cybersecuritynews.com/hackers-compromising-end-of-life-routers/
Hackers Arrested for Ransomware Attacks on Dutch Firms, Causing €4.5 Million in Damages	https://cybersecuritynews.com/hackers-arrested-for-ransomware-attacks/
Microsoft Teams To Block Screen Capture During Meetings	https://cybersecuritynews.com/microsoft-teams-block-screen-capture/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Chinese Hackers Exploit SAP RCE Vulnerability to Upload Supershell Backdoors	https://cybersecuritynews.com/chinese-hackers-exploit-sap-rce-vulnerability/
Hackers Attacking IT Admins by Poisoning SEO to Move Malware on Top of Search Results	https://cybersecuritynews.com/hackers-attacking-it-admins-by-poisoning-seo/
New Supply Chain Attack Targets Legitimate npm Package with 45,000 Weekly Downloads	https://cybersecuritynews.com/new-supply-chain-attack-targets-legitimate-npm-package/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Hackers Exploiting Output Messenger 0-Day Vulnerability to Deploy Malicious Payloads	**https://cybersecuritynews.com/output-messenger-0-day-vulnerability/**
VMware Tools Vulnerability Let Attackers Tamper Files to Trigger Malicious Operations	https://cybersecuritynews.com/vmware-tools-vulnerability/
SAP NetWeaver Vulnerability Exploited in Wild by Chinese Hackers	https://cybersecuritynews.com/sap-netweaver-vulnerability-exploited/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Apple Security Update: 8 Vulnerabilities Exposing Sensitive Data Patched	**https://cybersecuritynews.com/apple-security-update-sensitive-data/**
Linux Firewall IPFire 2.29 Core Update 194 Released with Security Enhancements	**https://cybersecuritynews.com/linux-firewall-ipfire-2-29-core-update-194/**

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Defendnot — A New Tool That Disables Windows Defender by Posing as an Antivirus Solution	https://cybersecuritynews.com/defendnot-disables-windows-defender/
"PupkinStealer" A New .NET-Based Malware Steals Browser Credentials & Exfiltrate via Telegram	https://cybersecuritynews.com/pupkinstealer-a-new-net-based-malware-steals-browser-credentials-exfiltrate-via-telegram/
Beware! Fake AI Video Generation Platforms Drop Stealer Malware on Your Computers	https://cybersecuritynews.com/beware-fake-ai-video-generation-platforms-drop-stealer-malware-on-your-computers/
Malicious Python Package Mimic as Attacking Discord Developers With Malicious Remote Commands	https://cybersecuritynews.com/malicious-python-package-mimic-as-attacking-discord-developers/
New Mamona Ransomware Attack Windows Machines by Abusing Ping Commands	https://cybersecuritynews.com/mamona-ransomware-attack-windows-machines/
Scattered Spider Malware Targeting Klaviyo, HubSpot, and Pure Storage Services	https://cybersecuritynews.com/scattered-spider-malware-targeting-klaviyo/
Threat Actors Using Multimedia Systems Via Stealthy Vishing Attack	https://cybersecuritynews.com/threat-actors-using-multimedia-systems/
Hackers Using Windows Remote Management to Stealthily Navigate Active Directory Network	https://cybersecuritynews.com/windows-remote-management-leveraged/
Hackers Weaponizing PDF Invoices to Attack Windows, Linux & macOS Systems	https://cybersecuritynews.com/hackers-weaponizing-pdf-invoices/
Critical Azure & Power Apps Vulnerabilities Let Attackers Escalate Privileges	https://cybersecuritynews.com/critical-azure-power-apps-vulnerabilities/
Hackers Attacking Windows IIS Web Server With Native Module Malware	https://cybersecuritynews.com/windows-iis-web-server-attacked/
Azure Storage Utility Vulnerability Let Attackers Escalate Their Privileges to Root	https://cybersecuritynews.com/azure-storage-utility-vulnerability/
Nitrogen Ransomware Exploits Antirootkit Driver File to Disable AV & EDR Tools	https://cybersecuritynews.com/nitrogen-ransomware-disable-av-edr-tools/
Lumma Stealer Evolves with New PowerShell Tools & Advanced Techniques	https://cybersecuritynews.com/lumma-stealer-evolves-with-new-powershell-tools/
Kimsuky Hacker Group Employs New Phishing Tactics & Malware Infections	https://cybersecuritynews.com/kimsuky-hacker-group-employs-new-phishing-tactics/
Hackers Leverage JPG Images to Execute Fully Undetectable Ransomware	https://cybersecuritynews.com/hackers-leverage-jpg-images/
Hackers Exploiting Legacy Protocols in Microsoft Entra ID to Bypass MFA & Conditional Access	https://cybersecuritynews.com/hackers-exploiting-legacy-protocols-in-microsoft-entra-id/
Hackers Exploit Copilot AI for SharePoint to Access Passwords & Other Sensitive Data	https://cybersecuritynews.com/hackers-exploit-copilot-ai-for-sharepoint/
Defendnot — A New Tool That Disables Windows Defender by Posing as an Antivirus Solution	https://cybersecuritynews.com/defendnot-disables-windows-defender/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
5 Must-Have Security Features for Native Apps	https://cybersecuritynews.com/security-features-for-native-apps/
Microsoft Releases Detailed Guide to Fix Windows Blue Screen Errors	https://cybersecuritynews.com/microsoft-releases-detailed-guide-to-fix/

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/