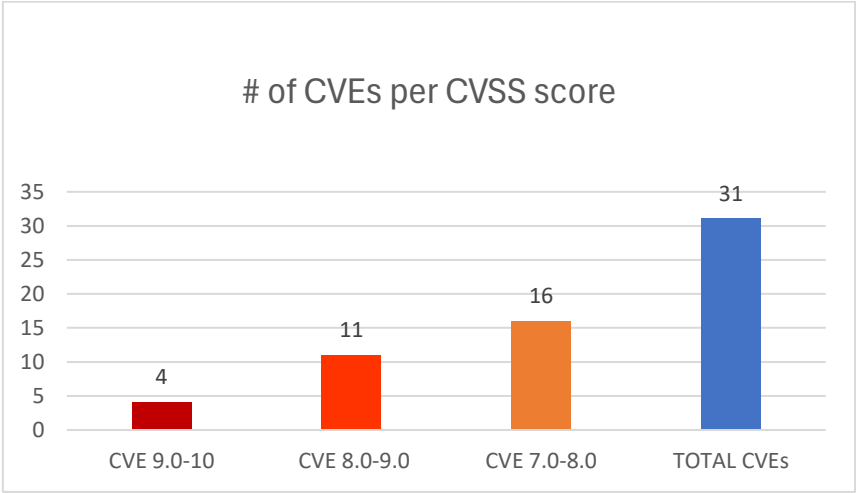
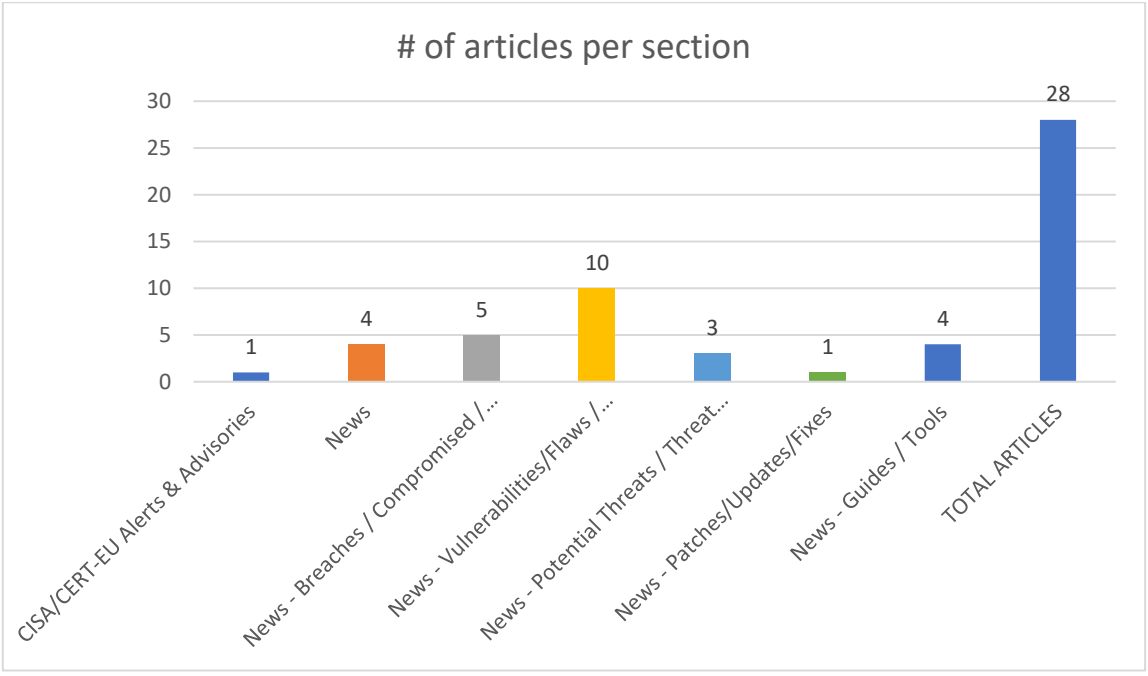
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 12/07/2025 - 15/07/2025





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-2025-7451	9,8	The iSherlock	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://www.twcert.org.tw/en/cp-139-10238-f2bba-2.html https://www.twcert.org.tw/tw/cp-132-10237-9e0f7-1.html
https://nvd.nist.gov/vuln/detail/CVE-2020-36849	9,8	The AIT CSV import/export plugin for WordPress	Unrestricted Upload of File with Dangerous Type	versions up to, and including, 3.0.3	https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/http/wp_ait_csv_rce.rb https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/http/wp_ait_csv_rce.rb https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/multi/http/wp_ait_csv_rce.rb https://wpscan.com/vulnerability/36e699a4-91f2-426d-ba14-26036fbfeaea https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-ait-themes-csv-import-export-arbitrary-file-upload-3-0-3/ https://www.ait-themes.club/wordpress-plugins/csv-import-export/ https://www.wordfence.com/threat-intel/vulnerabilities/id/cece751c-400d-42b4-9438-950d5aca51fc?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2020-36847	9,8	The Simple-File-List Plugin for WordPress	Unrestricted Upload of File with Dangerous Type	versions up to, and including, 4.2.2	https://packetstormsecurity.com/files/160221/ https://plugins.trac.wordpress.org/changeset/2286920/simple-file-list https://wpscan.com/vulnerability/365da9c5-a8d0-45f6-863c-1b1926ffd574/ https://wpscan.com/vulnerability/365da9c5-a8d0-45f6-863c-1b1926ffd574/ https://www.cybersecurity-help.cz/vdb/SB2020042711 https://www.wordfence.com/threat-intel/vulnerabilities/id/9eb835fd-6ebf-4162-856c-0366b663a07e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-38648	9,0	Ivanti DSM	Use of Hard-coded Credentials	before 2024.2	Resource https://forums.ivanti.com/s/article/SA-2024-07-12-CVE-2024-38648

https://nvd.nist.gov/vuln/detail/CVE-2025-7598	8,8	Tenda	Stack-based Buffer Overflow	AX1803 1.0.0.1	https://github.com/panda666-888/vuls/blob/main/tenda/ax1803/formSetWifiMacFilterCfg.md https://github.com/panda666-888/vuls/blob/main/tenda/ax1803/formSetWifiMacFilterCfg.md#poc https://vuldb.com/?ctiid.316297 https://vuldb.com/?id.316297 https://vuldb.com/?submit.615269 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-7586	8,8	Tenda	Stack-based Buffer Overflow	AC500 2.0.1.9(1307)	https://github.com/panda666-888/vuls/blob/main/tenda/ac500/formSetAPCfg.md https://github.com/panda666-888/vuls/blob/main/tenda/ac500/formSetAPCfg.md#poc https://vuldb.com/?ctiid.316285 https://vuldb.com/?id.316285 https://vuldb.com/?submit.615169 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-7571	8,8	UTT HiPER 840G	Improper Restriction of Operations within the Bounds of a Memory Buffer	up to 3.1.1-190328	https://github.com/d2pq/cve/blob/main/616/6.md https://github.com/d2pq/cve/blob/main/616/6.md#poc https://vuldb.com/?ctiid.316269 https://vuldb.com/?id.316269 https://vuldb.com/?submit.607747
https://nvd.nist.gov/vuln/detail/CVE-2025-7620	8,8	Digitware System Integration Corporation	Download of Code Without Integrity Check		https://www.twcert.org.tw/en/cp-139-10242-5ab42-2.html https://www.twcert.org.tw/tw/cp-132-10241-2ec07-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-7619	8,8	BatchSignCS	Relative Path Traversal		https://www.twcert.org.tw/en/cp-139-10240-00f86-2.html https://www.twcert.org.tw/tw/cp-132-10239-770ab-1.html

https://nvd.nist.gov/vuln/detail/CVE-2025-7551	8,8	Tenda	Stack-based Buffer Overflow	FH1201 1.2.0.14(408)	https://github.com/panda666-888/vuls/blob/main/tenda/fh1201/fromPptpUserAdd_modino.md https://github.com/panda666-888/vuls/blob/main/tenda/fh1201/fromPptpUserAdd_modino.md https://github.com/panda666-888/vuls/blob/main/tenda/fh1201/fromPptpUserAdd_modino.md#poc https://github.com/panda666-888/vuls/blob/main/tenda/fh1201/fromPptpUserAdd_modino.md#poc https://vuldb.com/?ctiid.316249 https://vuldb.com/?id.316249 https://vuldb.com/?submit.614975 https://vuldb.com/?submit.614976 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-7505	8,8	Tenda	Stack-based Buffer Overflow	FH451 1.0.0.9	https://github.com/zezhifu1/cve_report/blob/main/FH451/frmL7ProtForm.md https://github.com/zezhifu1/cve_report/blob/main/FH451/frmL7ProtForm.md#payload https://vuldb.com/?ctiid.316188 https://vuldb.com/?id.316188 https://vuldb.com/?submit.611504 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-6423	8,8	The BeeTeam368 Extensions plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 2.3.5	https://themeforest.net/item/vidmov-video-wordpress-theme/35542187#item-description__change-log https://www.wordfence.com/threat-intel/vulnerabilities/id/96170b82-6ed9-4a52-8592-944163cdd3cf?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7460	8,8	TOTOLINK	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	T6 4.1.5cu.748_B20211015	https://github.com/ElvisBlue/Public/blob/main/Vuln/1.md https://github.com/ElvisBlue/Public/blob/main/Vuln/1.md#poc https://github.com/ElvisBlue/Public/blob/main/Vuln/1.md#poc https://vuldb.com/?ctiid.316111 https://vuldb.com/?id.316111 https://vuldb.com/?submit.609819 https://www.totolink.net/

https://nvd.nist.gov/vuln/detail/CVE-2025-6057	8,8	The WPBookit plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 1.0.4	https://plugins.trac.wordpress.org/browser/wpbookit/trunk/core/admin/classes/controllers/class.wpb-profile-controller.php#L85 https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3326098%40wpbookit&new=3326098%40wpbookit&sfp_email=&sfph_mail= https://wordpress.org/plugins/wpbookit/ https://www.wordfence.com/threat-intel/vulnerabilities/id/fac81cc0-c6c9-4009-aacb-52adc70c0261?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-1313	8,8	The Nokri - Job Board WordPress Theme theme for WordPress	Authentication Bypass Using an Alternate Path or Channel	all versions up to, and including, 1.6.3	https://themeforest.net/item/nokri-job-board-wordpress-theme/22677241 https://www.wordfence.com/threat-intel/vulnerabilities/id/507c2abd-47d3-4a28-a9b7-a1ad9b026e7d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2020-36848	7,5	The Total Upkeep – WordPress Backup Plugin plus Restore & Migrate by BoldGrid plugin for WordPress	Exposure of Sensitive Information to an Unauthorized Actor	all versions up to, and including, 1.14.9	https://plugins.trac.wordpress.org/changeset/2439376/boldgrid-backup https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/auxiliary/scanner/http/wp_total_upkeep_downloader.rb https://wpscan.com/vulnerability/d35c19d9-8586-4c5b-9a01-44739cbeee19/ https://www.wordfence.com/threat-intel/vulnerabilities/id/86a5adaf-02b7-4b42-a048-8bc01f07656b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7504	7,5	The Friends plugin for WordPress	Deserialization of Untrusted Data	version 3.5.1	https://drive.google.com/file/d/1K-_AcDk9BhUa0kSQ_M-UUnLgmnYJTA0l/view https://github.com/akirk/friends/pull/537 https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3306684%40friends&new=3306684%40friends&sfp_email=&sfph_mail= https://wordpress.org/plugins/friends/ https://www.wordfence.com/threat-intel/vulnerabilities/id/cf91d75e-cef4-4154-aa16-6ca96db9c5bb?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7594	7,3	Job Diary	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/yihaofuweng/cve/issues/20 https://vuldb.com/?ctiid.316293 https://vuldb.com/?id.316293 https://vuldb.com/?submit.615239

https://nvd.nist.gov/vuln/detail/CVE-2025-7587	7,3	Online Appointment Booking System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/BalanceLee/CVE/issues/1 https://vuldb.com/?ctiid.316286 https://vuldb.com/?id.316286 https://vuldb.com/?submit.615212 https://vuldb.com/?submit.615377
https://nvd.nist.gov/vuln/detail/CVE-2025-7547	7,3	Campcodes Online Movie Theater Seat Reservation System	Improper Access Control	1.0	https://github.com/N1n3b9S/cve/issues/1 https://github.com/N1n3b9S/cve/issues/1 https://vuldb.com/?ctiid.316245 https://vuldb.com/?id.316245 https://vuldb.com/?submit.614466 https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-7542	7,3	PHPGurukul User Registration & Login and User Management System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	3.3	https://github.com/4m3rr0r/PoCVulDb/blob/main/CVE-2025-7542.md https://phpgurukul.com/ https://vuldb.com/?ctiid.316238 https://vuldb.com/?id.316238 https://vuldb.com/?submit.613919
https://nvd.nist.gov/vuln/detail/CVE-2025-7539	7,3	Online Appointment Booking System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/bit001020/cve/issues/3 https://vuldb.com/?ctiid.316235 https://vuldb.com/?id.316235 https://vuldb.com/?submit.613689
https://nvd.nist.gov/vuln/detail/CVE-2025-7534	7,3	PHPGurukul Student Result Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2.0	https://github.com/4m3rr0r/PoCVulDb/blob/main/CVE-2025-7534.md https://github.com/4m3rr0r/PoCVulDb/blob/main/CVE-2025-7534.md https://phpgurukul.com/ https://vuldb.com/?ctiid.316230 https://vuldb.com/?id.316230 https://vuldb.com/?submit.613168

https://nvd.nist.gov/vuln/detail/CVE-2025-7523	7,3	Jinher OA	Improper Restriction of XML External Entity Reference	1.0	https://github.com/BigMancer/Jinhe-OA-XXE-Vulnerability https://github.com/BigMancer/Jinhe-OA-XXE-Vulnerability?tab=readme-ov-file#proof-of-concept https://vuldb.com/?ctiid.316220 https://vuldb.com/?id.316220 https://vuldb.com/?submit.611183
https://nvd.nist.gov/vuln/detail/CVE-2025-7521	7,3	PHPGurukul Vehicle Parking Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.13	https://github.com/f1rstb100d/myCVE/issues/122 https://phpgurukul.com/ https://vuldb.com/?ctiid.316218 https://vuldb.com/?id.316218 https://vuldb.com/?submit.610579
https://nvd.nist.gov/vuln/detail/CVE-2025-7514	7,3	Modern Bag	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/haoyv147/cve/issues/1 https://github.com/haoyv147/cve/issues/1 https://vuldb.com/?ctiid.316196 https://vuldb.com/?id.316196 https://vuldb.com/?submit.612709
https://nvd.nist.gov/vuln/detail/CVE-2025-7466	7,3	ABC Courier Management	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/kensei0x/cve/issues/2 https://github.com/kensei0x/cve/issues/2 https://vuldb.com/?ctiid.316118 https://vuldb.com/?id.316118 https://vuldb.com/?submit.610390
https://nvd.nist.gov/vuln/detail/CVE-2025-7459	7,3	Mobile Shop	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ https://github.com/xiajian-qx/cve-xiajian/issues/1 https://github.com/xiajian-qx/cve-xiajian/issues/1 https://vuldb.com/?ctiid.316108 https://vuldb.com/?id.316108 https://vuldb.com/?submit.609657
https://nvd.nist.gov/vuln/detail/CVE-2025-5199	7,3	Canonical Multipass	Incorrect Default Permissions	up to and including version 1.15.1 on macOS	https://github.com/canonical/multipass/pull/4115 https://github.com/canonical/multipass/security/advisories/GHSA-2j82-p5cq-62p3 https://github.com/canonical/multipass/security/advisories/GHSA-2j82-p5cq-62p3

https://nvd.nist.gov/vuln/detail/CVE-2024-58258	7,2	SugarCRM	Improper Control of Generation of Code ('Code Injection')	before 13.0.4 and 14.x before 14.0.1	https://support.sugarcrm.com/resources/security/sugarcrm-sa-2024-059/
https://nvd.nist.gov/vuln/detail/CVE-2025-1384	7,0	the NJ/NX-series Machine Automation Controllers and the Sysmac Studio Software	Least Privilege Violation		https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2025-004_en.pdf https://www.fa.omron.co.jp/product/security/assets/pdf/ja/OMSR-2025-004_ja.pdf

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-47812 Wing FTP Server Improper Neutralization of Null Byte or NUL Character Vulnerability	https://www.cisa.gov/news-events/alerts/2025/07/14/cisa-adds-one-known-exploited-vulnerability-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
Inorganic DNA: How nanoparticles could be the future of anti-counterfeiting tech	https://www.helpnetsecurity.com/2025/07/15/inorganic-dna-nanoparticles-anti-counterfeiting-tech/
MITRE Launches AADAPT Framework for Detecting and Responding to Digital Asset Management Attacks	https://cybersecuritynews.com/mitre-aadapt/
Fake News Sites Mimicking CNN, BBC and CNBC Pave Way for Investment Scams	https://www.infosecurity-magazine.com/news/fake-news-sites-investment-scams/
20-Year-Old Vulnerability Allows Hackers to Control Train Brakes	https://cybersecuritynews.com/hackers-control-train-brakes/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Nippon Steel Hit by Zero-Day Attack, Sensitive Data Believed Stolen	https://dailysecurityreview.com/security-spotlight/nippon-steel-hit-by-zero-day-attack-sensitive-data-believed-stolen/
Global Louis Vuitton data breach impacts UK, South Korea, and Turkey	https://securityaffairs.com/179908/data-breach/global-louis-vuitton-data-breach-impacts-uk-south-korea-and-turkey.html
Malicious VSCode extension in Cursor IDE led to $500K crypto theft	https://www.bleepingcomputer.com/news/security/malicious-vscode-extension-in-cursor-ide-led-to-500k-crypto-theft/
McDonald's job app exposes data of 64 Million applicants	https://securityaffairs.com/179840/hacking/mcdonalds-job-app-exposes-data-of-64-million-applicants.html
Dordt University notifies 34K+ people of April 2024 data breach that compromised SSNs, medical info	https://www.comparitech.com/news/dordt-university-notifies-34k-people-of-april-2024-data-breach-that-compromised-ssns-medical-info/?&web_view=true

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Google Gemini flaw hijacks email summaries for phishing	https://www.bleepingcomputer.com/news/security/google-gemini-flaw-hijacks-email-summaries-for-phishing/
Critical Vulnerability Exposes Fortinet FortiWeb to Full Takeover (CVE-2025-25257)	https://hackread.com/critical-vulnerability-fortinet-fortiweb-cve-2025-25257/
Wing FTP Server flaw actively exploited shortly after technical details were made public	https://securityaffairs.com/179861/hacking/wing-ftp-server-flaw-actively-exploited-shortly-after-technical-details-were-made-public.html
Meta's Llama Firewall Bypassed Using Prompt Injection Vulnerability	https://cybersecuritynews.com/metas-llama-firewall/
Patch immediately: CVE-2025-25257 PoC enables remote code execution on Fortinet FortiWeb	https://securityaffairs.com/179874/security/patch-immediately-cve-2025-25257-poc-enables-remote-code-execution-on-fortinet-fortiweb.html
eSIM Vulnerability in Kigen's eUICC Cards Exposes Billions of IoT Devices to Malicious Attacks	https://thehackernews.com/2025/07/esim-vulnerability-in-kigens-euicc.html
Wing FTP Server Under Active Exploitation Following Critical RCE Vulnerability Disclosure	https://dailysecurityreview.com/security-spotlight/wing-ftp-server-under-active-exploitation-following-critical-rce-vulnerability-disclosure/
RenderShock 0-Click Vulnerability Executes Payloads via Background Process Without User Interaction	https://cybersecuritynews.com/rendershock-0-click-vulnerability/
Gigabyte UEFI Firmware Vulnerability Let Attackers Execute Arbitrary Code in the SMM Environment	https://cybersecuritynews.com/gigabyte-uefi-firmware-vulnerability/
Critical Vulnerabilities Discovered in Adobe Acrobat Reader and ASUS Armoury Crate	https://dailysecurityreview.com/security-spotlight/critical-vulnerabilities-discovered-in-adobe-acrobat-reader-and-asus-armoury-crate/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Windows 10 KB5062554 update breaks emoji panel search feature	https://www.bleepingcomputer.com/news/microsoft/windows-10-kb5062554-update-breaks-emoji-panel-search-feature/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Interlock Ransomware Unleashes New RAT in Widespread Campaign	https://www.infosecurity-magazine.com/news/interlock-ransomware-new-rat/
GPUHammer: New RowHammer Attack Variant Degrades AI Models on NVIDIA GPUs	https://thehackernews.com/2025/07/gpuhammer-new-rowhammer-attack-variant.html
Google Gemini AI Bug Allows Invisible, Malicious Prompts	https://www.darkreading.com/remote-workforce/google-gemini-ai-bug-invisible-malicious-prompts

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	**https://cybersecuritynews.com/enterprise-security-monitoring-tools/**
10 Best Cloud VPN Providers – 2025	https://cybersecuritynews.com/best-cloud-vpn/
Top 11 Passwordless Authentication Tools – 2025	https://cybersecuritynews.com/passwordless-authentication/
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/ 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/