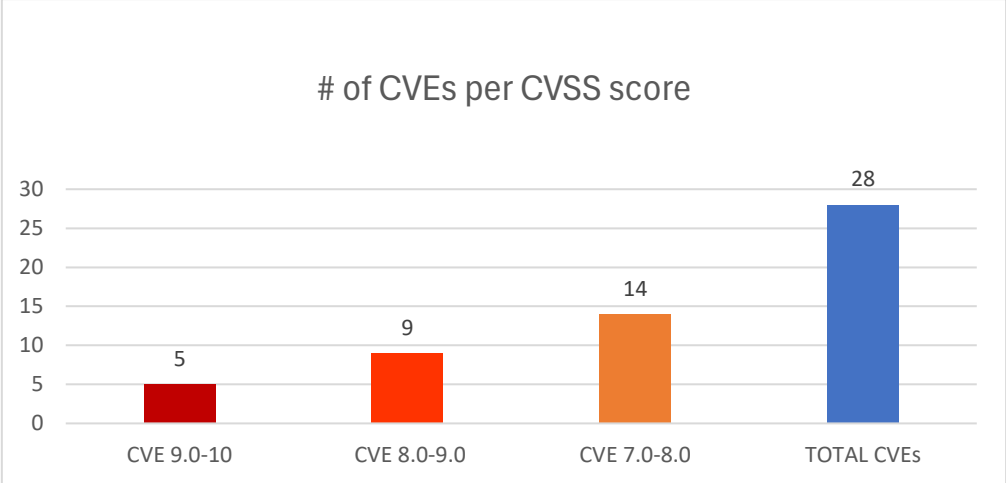
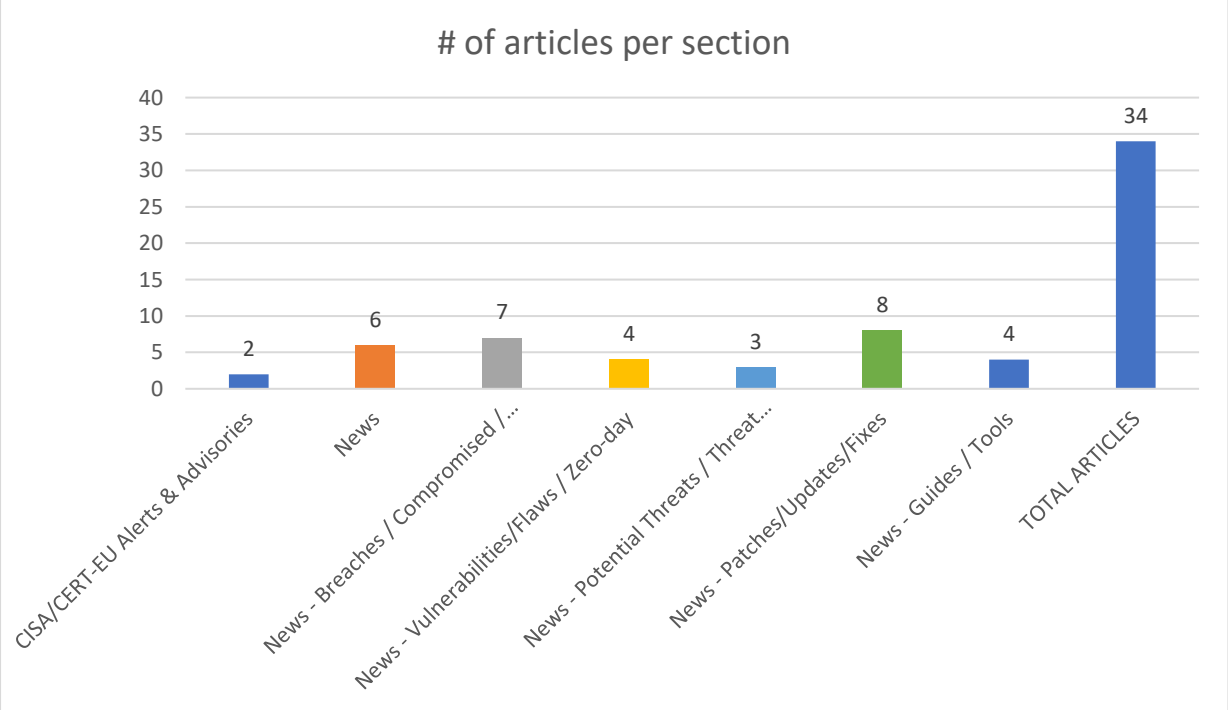
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 14/05/2025 - 16/05/2025





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-2025-47781	**9,8**	Rallly	Insufficient Entropy	Versions up to and including 3.22.1	https://github.com/lukevella/rallly/security/advisories/GHSA-gm8g-3r3j-48hv https://github.com/lukevella/rallly/security/advisories/GHSA-gm8g-3r3j-48hv
https://nvd.nist.gov/vuln/detail/CVE-2024-24780	**9,8**	Apache IoTDB	Improper Control of Generation of Code ('Code Injection')	from 1.0.0 before 1.3.4	http://www.openwall.com/lists/oss-security/2025/05/14/2 https://lists.apache.org/thread/xphtm98v3zsk9vlpfh481m1ry2ctxvmj
https://nvd.nist.gov/vuln/detail/CVE-2025-47777	**9,6**	5ire	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Versions prior to 0.11.1	https://github.com/nanbingxyz/5ire/commit/56601e012095194a4be0d4cb6da6b5b3cb53dea8 https://github.com/nanbingxyz/5ire/security/advisories/GHSA-mr8w-mmvv-6hq8 https://positive.security/blog/url-open-rce https://shabarkin.notion.site/1-click-RCE-in-Electron-Applications-501c2e96e7934610979cd3c72e844a22 https://www.electronjs.org/docs/latest/tutorial/security https://www.youtube.com/watch?v=ROFYhS9E9eU

https://nvd.nist.gov/vuln/detail/CVE-2025-43567	**9,3**	Adobe Connect	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	versions 12.8 and earlier	https://helpx.adobe.com/security/products/connect/apsb25-36.html
https://nvd.nist.gov/vuln/detail/CVE-2025-43564	**9,1**	ColdFusion	Incorrect Authorization	versions 2025.1, 2023.13, 2021.19	https://helpx.adobe.com/security/products/coldfusion/apsb25-52.html
https://nvd.nist.gov/vuln/detail/CVE-2024-54780	**8,8**	Netgate pfSense CE	Improper Control of Generation of Code ('Code Injection')	prior to 2.8.0 beta release	http://netgate.com https://blog.brillantit.com/exploiting-pfsense-xss-command-injection-cloud-hijack/
https://nvd.nist.gov/vuln/detail/CVE-2024-54780	**8,8**	Netgate pfSense CE	Improper Control of Generation of Code ('Code Injection')	prior to 2.8.0 beta release	http://netgate.com https://blog.brillantit.com/exploiting-pfsense-xss-command-injection-cloud-hijack/
https://nvd.nist.gov/vuln/detail/CVE-2025-30663	**8,8**	Zoom Workplace Apps	Time-of-check Time-of-use (TOC-TOU) Race Condition	-	https://www.zoom.com/en/trust/security-bulletin/zsb-25016
https://nvd.nist.gov/vuln/detail/CVE-2025-24022	**8,5**	iTop	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to versions 2.7.12, 3.1.3, and 3.2.1	https://github.com/Combodo/iTop/security/advisories/GHSA-rhv2-wfrr-4j2j
https://nvd.nist.gov/vuln/detail/CVE-2025-20003	**8,2**	Intel(R) Graphics Driver	Improper Link Resolution Before File Access ('Link Following')	-	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01259.html

https://nvd.nist.gov/vuln/detail/CVE-2025-3623	**8,1**	The Uncanny Automator plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 6.4.0.1	https://automator-plugin.com/knowledge-base/uncanny-automator-changelog/#6-4-0-2-2025-04-18 https://plugins.trac.wordpress.org/browser/uncanny-automator/trunk/src/core/lib/helpers/class-automator-recipe-helpers.php#L540 https://plugins.trac.wordpress.org/changeset/3276577/uncanny-automator/trunk/src/core/lib/helpers/class-automator-recipe-helpers.php https://wordpress.org/plugins/uncanny-automator/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/00bcfd8f-9785-449a-a0ea-16e2583d684a?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-3623	**8,1**	The Uncanny Automator plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 6.4.0.1	https://automator-plugin.com/knowledge-base/uncanny-automator-changelog/#6-4-0-2-2025-04-18 https://plugins.trac.wordpress.org/browser/uncanny-automator/trunk/src/core/lib/helpers/class-automator-recipe-helpers.php#L540 https://plugins.trac.wordpress.org/changeset/3276577/uncanny-automator/trunk/src/core/lib/helpers/class-automator-recipe-helpers.php https://wordpress.org/plugins/uncanny-automator/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/00bcfd8f-9785-449a-a0ea-16e2583d684a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3834	**8,1**	Zohocorp ManageEngine ADAudit Plus	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	versions 8510 and prior	https://www.manageengine.com/products/active-directory-audit/cve-2025-3834.html
https://nvd.nist.gov/vuln/detail/CVE-2025-26646	**8**	.NET, Visual Studio	External Control of File Name or Path	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26646
https://nvd.nist.gov/vuln/detail/CVE-2025-3931	**7,8**	Yggdrasil	Improper Handling of Insufficient Permissions or Privileges	-	https://access.redhat.com/errata/RHSA-2025:7592 https://access.redhat.com/security/cve/CVE-2025-3931 https://bugzilla.redhat.com/show_bug.cgi?id=2362345

https://nvd.nist.gov/vuln/detail/CVE-2025-43572	**7,8**	Dimension	Out-of-bounds Write	versions 4.1.2 and earlier	https://helpx.adobe.com/security/products/dimension/apsb25-45.html
https://nvd.nist.gov/vuln/detail/CVE-2025-43571	**7,8**	Substance3D - Stager	Use After Free	versions 3.1.1 and earlier	https://helpx.adobe.com/security/products/substance3d_stager/apsb25-46.html
https://nvd.nist.gov/vuln/detail/CVE-2025-22843	**7,8**	Edge Orchestrator software for Intel(R) Tiber™	Incorrect Execution-Assigned Permissions	-	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01239.html
https://nvd.nist.gov/vuln/detail/CVE-2025-43554	**7,8**	Substance3D - Modeler	Out-of-bounds Write	versions 1.21.0 and earlier	https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-51.html
https://nvd.nist.gov/vuln/detail/CVE-2025-20008	**7,7**	Intel(R) Simics(R) Package Manager software	Insecure Inherited Permissions	before version 1.12.0	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01297.html
https://nvd.nist.gov/vuln/detail/CVE-2025-3600	**7,5**	Progress® Telerik® UI for AJAX	Uncontrolled Resource Consumption	versions 2011.2.712 to 2025.1.218	https://www.telerik.com/products/aspnet-ajax/documentation/knowledge-base/kb-security-unsafe-reflection-cve-2025-3600
https://nvd.nist.gov/vuln/detail/CVE-2025-21094	**7,5**	UEFI firmware DXE module	Improper Input Validation	Intel(R) Server D50DNP and M50FCP	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01269.html
https://nvd.nist.gov/vuln/detail/CVE-2025-47445	**7,5**	Themewinter Eventin	Relative Path Traversal	from n/a through 4.0.26	https://patchstack.com/database/wordpress/plugin/wp-event-solution/vulnerability/wordpress-eventin-4-0-26-arbitrary-file-download-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-20006	**7,4**	Intel(R) PRO-Set/Wireless WiFi Software for Windows	Use After Free	before version 23.100	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01270.html

https://nvd.nist.gov/vuln/detail/CVE-2025-20052	**7,3**	Intel(R) Graphics software	Improper Access Control	-	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01259.html
https://nvd.nist.gov/vuln/detail/CVE-2024-36292	**7,3**	Intel(R) Data Center GPU Flex Series for Windows driver	Improper Restriction of Operations within the Bounds of a Memory Buffer	before version 31.0.101.4314	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01253.html
https://nvd.nist.gov/vuln/detail/CVE-2025-40595	**7,2**	SMA1000 Appliance Work Place interface	Server-Side Request Forgery (SSRF)	-	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0010
https://nvd.nist.gov/vuln/detail/CVE-2025-20004	**7,2**	Intel(R) Xeon(R) 6 processor E-Cores	Insufficient Control Flow Management	-	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01273.html

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2024-12987 DrayTek Vigor Routers OS Command Injection Vulnerability ▪ CVE-2025-4664 Google Chromium Loader Insufficient Policy Enforcement Vulnerability ▪ CVE-2025-42999 SAP NetWeaver Deserialization Vulnerability	https://www.cisa.gov/news-events/alerts/2025/05/15/cisa-adds-three-known-exploited-vulnerabilities-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-32756 Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability	https://www.cisa.gov/news-events/alerts/2025/05/14/cisa-adds-one-known-exploited-vulnerability-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
INE Security Alert: Continuous CVE Practice Closes Critical Gap Between Vulnerability Alerts and Effective Defense	https://hackread.com/ine-security-alert-continuous-cve-practice-closes-critical-gap-between-vulnerability-alerts-and-effective-defense/
U.S. CISA adds Microsoft Windows flaws to its Known Exploited Vulnerabilities catalog	https://securityaffairs.com/177856/security/u-s-cisa-adds-microsoft-windows-flaws-to-its-known-exploited-vulnerabilities-catalog.html
#Infosec2025: Ransomware Enters 'Post-Trust Ecosystem,' NCA Cyber Expert Says	https://www.infosecurity-magazine.com/news/ransomware-enters-posttrust/
Leak confirms OpenAI's ChatGPT will integrate MCP	https://www.bleepingcomputer.com/news/artificial-intelligence/leak-confirms-openais-chatgpt-will-integrate-mcp/
Microsoft Outlook Down – Millions of Users Affected With This Longest Outage in Microsoft History	https://cybersecuritynews.com/microsoft-outlook-down/
Enisa Launches European Vulnerability Database to Enhance Digital Security	https://cybersecuritynews.com/enisa-launches-euvd/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Fashion giant Dior discloses cyberattack, warns of data breach	https://www.bleepingcomputer.com/news/security/fashion-giant-dior-discloses-cyberattack-warns-of-data-breach/
Australian Human Rights Commission leaks docs to search engines	https://www.bleepingcomputer.com/news/security/australian-human-rights-commission-leaks-docs-to-search-engines/
Government webmail hacked via XSS bugs in global spy campaign	https://www.bleepingcomputer.com/news/security/government-webmail-hacked-via-xss-bugs-in-global-spy-campaign/
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/
Coinbase disclosed a data breach after an extortion attempt	https://securityaffairs.com/177878/cyber-crime/coinbase-disclosed-a-data-breach-after-an-extortion-attempt.html
HireClick Exposes 5.7 Million Resume Files Due to Misconfigured Cloud Storage	https://dailysecurityreview.com/security-spotlight/hireclick-exposes-5-7-million-resume-files-due-to-misconfigured-cloud-storage/
Nova Scotia Power discloses data breach after March security incident	https://securityaffairs.com/177887/cyber-crime/nova-scotia-power-discloses-data-breach-after-march-security-incident.html

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Researchers Expose New Intel CPU Flaws Enabling Memory Leaks and Spectre v2 Attacks	https://thehackernews.com/2025/05/researchers-expose-new-intel-cpu-flaws.html
Samsung Patches CVE-2025-4632 Used to Deploy Mirai Botnet via MagicINFO 9 Exploit	https://thehackernews.com/2025/05/samsung-patches-cve-2025-4632-used-to.html
SonicWall SMA1000 Vulnerability Let Attackers to Exploit Encoded URLs To Gain Internal Systems Access Remotely	https://cybersecuritynews.com/sonicwall-sma1000-vulnerability/
Hackers Abuse Google Services to Send Malicious Law Enforcement Requests	https://cybersecuritynews.com/hackers-abuse-google-services/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Google fixed a Chrome vulnerability that could lead to full account takeover	https://securityaffairs.com/177899/security/google-fixed-a-chrome-vulnerability-that-could-lead-to-full-account-takeover.html
Microsoft Fixes 78 Flaws, 5 Zero-Days Exploited; CVSS 10 Bug Impacts Azure DevOps Server	https://thehackernews.com/2025/05/microsoft-fixes-78-flaws-5-zero-days.html
Microsoft Fixes Seven Zero-Days in May Patch Tuesday	https://www.infosecurity-magazine.com/news/microsoft-seven-zerodays-may-patch/
Microsoft fixes Linux boot issues on dual-boot Windows systems	https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-linux-boot-issues-on-dual-boot-windows-systems/
Google fixes high severity Chrome flaw with public exploit	https://www.bleepingcomputer.com/news/security/google-fixes-high-severity-chrome-flaw-with-public-exploit/
Jenkins Security Update Released With the Fixes for the Vulnerabilities that Exploit CI/CD Pipelines	https://cybersecuritynews.com/jenkins-security-update/
Fortinet fixed actively exploited FortiVoice zero-day	https://securityaffairs.com/177800/security/fortinet-fixed-actively-exploited-fortivoice-zero-day.html
Ivanti Patches EPMM Vulnerabilities Exploited for Remote Code Execution in Limited Attacks	https://thehackernews.com/2025/05/ivanti-patches-epmm-vulnerabilities.html

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
SAP NetWeaver Flaw Exploited by Ransomware Groups and Chinese-Backed Hackers	https://www.infosecurity-magazine.com/news/sap-netweaver-vulnerability/
New .NET Multi-stage Loader Attacking Windows Systems to Deploy Malicious Payloads	https://cybersecuritynews.com/new-net-multi-stage-loader-attacking-windows-systems/
Threat Actors Weaponizing Open Source Packages to Deliver Malware in Supply Chain Attack	https://cybersecuritynews.com/threat-actors-weaponizing-open-source-packages/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best Cyber Attack Simulation Tools – 2025	https://cybersecuritynews.com/cyber-attack-simulation-tools/
The ultimate guide to SaaS identity security in 2025	https://thehackernews.uk/saas-identity-guide-25
10 Steps to Microsoft 365 Cyber Resilience	https://thehackernews.uk/m365-cyber-resilience-10
Top Cybersecurity Tools of 2025 To Managing Remote Device Threats	https://cybersecuritynews.com/top-cybersecurity-tools-managing-remote-device-threats/

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/