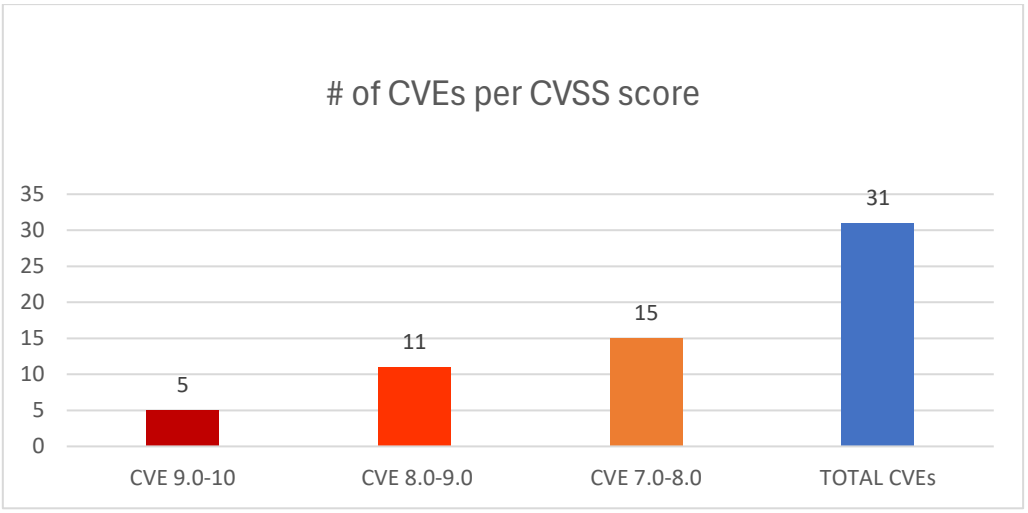
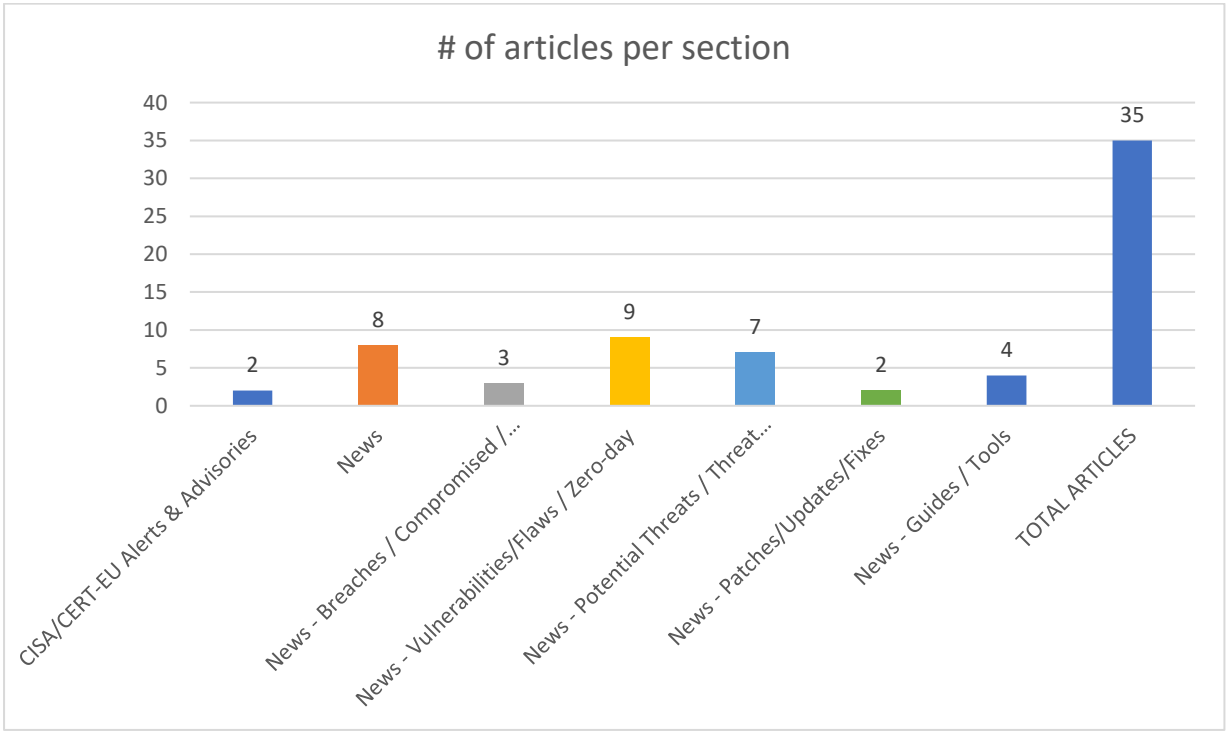
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 30/04/2025 - 02/05/2025





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-2025-30390	**9,9**	Azure	Improper Authorization	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30390
https://nvd.nist.gov/vuln/detail/CVE-2025-3709	**9,8**	Agentflow from Flowring Technology	Improper Restriction of Excessive Authentication Attempts	-	https://www.twcert.org.tw/en/cp-139-10090-112f7-2.html https://www.twcert.org.tw/tw/cp-132-10091-12462-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-3708	**9,8**	Le-show medical practice management system	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	-	https://www.twcert.org.tw/en/cp-139-10086-dbfd0-2.html https://www.twcert.org.tw/tw/cp-132-10085-69e16-1.html

https://nvd.nist.gov/vuln/detail/CVE-2025-3746	**9,8**	The OTP-less one tap Sign in plugin for WordPress	Missing Authorization	versions 2.0.14 to 2.0.59	https://plugins.trac.wordpress.org/browser/otpless/tags/2.0.59./includes/class-login.php https://www.wordfence.com/threat-intel/vulnerabilities/id/63fab608-1a75-4b07-8d82-8ab87e197547?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-30392	**9,8**	Azure Bot Framework SDK	Improper Authorization	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30392
https://nvd.nist.gov/vuln/detail/CVE-2024-13418	**8,8**	WordPress	Unrestricted Upload of File with Dangerous Type	various versions	https://themeforest.net/item/beyot-wordpress-real-estate-theme/19514964 https://www.wordfence.com/threat-intel/vulnerabilities/id/bced4547-3264-43dc-8bb1-89a06f74ccbd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-4150	**8,8**	Netgear EX6200	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	version 1.0.3.94	https://github.com/jylsec/vuldb/blob/main/Netgear/netgear_ex6200/Buffer_overflow-sub_54340-gui_region/README.md https://vuldb.com/?ctiid.306682 https://vuldb.com/?id.306682 https://vuldb.com/?submit.560804 https://www.netgear.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-4149	**8,8**	Netgear EX6200	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	version 1.0.3.94	https://github.com/jylsec/vuldb/blob/main/Netgear/netgear_ex6200/Buffer_overflow-sub_54014-gui_region/README.md https://vuldb.com/?ctiid.306681 https://vuldb.com/?id.306681 https://vuldb.com/?submit.560803 https://www.netgear.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-1305	**8,8**	The NewsBlogger theme for WordPress	Cross-Site Request Forgery (CSRF)	all versions up to, and including, 0.2.5.4	https://themes.trac.wordpress.org/browser/newsblogger/0.2/functions.php#L440 https://themes.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=269615%40newsblogger&new=269615%40newsblogger&sfp_email=&sfph_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/7b2cac27-4a36-490f-b2d8-3c6f32843a38?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-4139	**8,8**	Netgear EX6120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	versions 1.0.0.68	https://github.com/jylsec/vuldb/blob/main/Netgear/netgear_ex6120/Buffer_overflow-fwAcosCgiInboundport_end/README.md https://vuldb.com/?ctiid.306631 https://vuldb.com/?id.306631 https://vuldb.com/?submit.560785 https://www.netgear.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-4120	**8,8**	Netgear JWNR2000v2	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	version 1.0.0.11	https://github.com/jylsec/vuldb/blob/main/Netgear/netgear_JWNR2000v2/Buffer_overflow-sub_4238E8-log_type/README.md https://vuldb.com/?ctiid.306600 https://vuldb.com/?id.306600 https://vuldb.com/?submit.560774 https://www.netgear.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-30389	**8,7**	Azure Bot Framework SDK	Improper Authorization	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30389

https://nvd.nist.gov/vuln/detail/CVE-2025-21416	**8,5**	Azure Virtual Desktop		Missing Authorization	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21416
https://nvd.nist.gov/vuln/detail/CVE-2025-3952	**8,1**	The Projectopia – WordPress Project Management plugin for WordPress	Missing Authorization	all versions up to, and including, 5.1.16	https://plugins.trac.wordpress.org/browser/projectopia-core/trunk/includes/functions/admin/admin_functions.php#L838 https://plugins.trac.wordpress.org/changeset/3284330/ https://www.wordfence.com/threat-intel/vulnerabilities/id/de7489e8-fe18-4a80-832c-aa62424c538b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-2816	**8,1**	The Page View Count plugin for WordPress	Missing Authorization	in versions 2.8.0 to 2.8.4	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3282975%40page-views-count&new=3282975%40page-views-count&sfp_email=&sfph_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/e6fb9558-06e5-4297-93df-ee9a6971f0ec?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-30391	**8,1**	Microsoft Dynamics	Improper Input Validation	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30391
https://nvd.nist.gov/vuln/detail/CVE-2024-13344	**7,5**	The Advance Seat Reservation Management for WooCommerce plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 3.3	https://codecanyon.net/item/advance-seat-reservation-management-for-woocommerce/19984266 https://www.wordfence.com/threat-intel/vulnerabilities/id/35acdb85-e463-46b1-aea7-a6d4c3581499?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2024-13322	**7,5**	The Ads Pro Plugin - Multi-Purpose WordPress Advertising Manager plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 4.88	https://codecanyon.net/item/ads-pro-plugin-multipurpose-wordpress-advertising-manager/10275010 https://www.wordfence.com/threat-intel/vulnerabilities/id/3bcb60a8-220f-45a4-a9a9-10f64acf470c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-33074	**7,5**	Microsoft Azure Functions	Improper Verification of Cryptographic Signature	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33074
https://nvd.nist.gov/vuln/detail/CVE-2025-4179	**7,3**	The Flynax Bridge plugin for WordPress	Missing Authorization	all versions up to, and including, 2.2.0	https://plugins.trac.wordpress.org/browser/flynax-bridge/trunk/src/API.php#L288 https://www.wordfence.com/threat-intel/vulnerabilities/id/a2447cf4-0261-4ef2-98ec-98fa02dc8b87?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-4195	**7,3**	Gym Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/ARPANET-cybersecurity/vuldb/issues/6 https://itsourcecode.com/ https://vuldb.com/?ctiid.306808 https://vuldb.com/?id.306808 https://vuldb.com/?submit.561876
https://nvd.nist.gov/vuln/detail/CVE-2025-4193	**7,3**	Restaurant Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/ARPANET-cybersecurity/vuldb/issues/5 https://itsourcecode.com/ https://vuldb.com/?ctiid.306806 https://vuldb.com/?id.306806 https://vuldb.com/?submit.561849

https://nvd.nist.gov/vuln/detail/CVE-2025-4191	**7,3**	PHPGurukul Employee Record Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.3	https://github.com/ideal-valli/myCVE/issues/3 https://phpgurukul.com/ https://vuldb.com/?ctiid.306805 https://vuldb.com/?id.306805 https://vuldb.com/?submit.561816
https://nvd.nist.gov/vuln/detail/CVE-2025-4184	**7,3**	PCMan FTP Server	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	version 2.0.7	https://fitoxs.com/exploit/exploit-d8578edf8458ce06fbc5bb76a58c5ca4.txt https://vuldb.com/?ctiid.306801 https://vuldb.com/?id.306801 https://vuldb.com/?submit.561144
https://nvd.nist.gov/vuln/detail/CVE-2025-4176	**7,3**	PHPGurukul Blood Bank & Donor Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 2.4	https://github.com/bluechips-zhao/myCVE/issues/5 https://phpgurukul.com/ https://vuldb.com/?ctiid.306796 https://vuldb.com/?id.306796 https://vuldb.com/?submit.561764
https://nvd.nist.gov/vuln/detail/CVE-2025-4174	**7,3**	PHPGurukul COVID19 Testing Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/FLYFISH567/CVE/issues/1 https://phpgurukul.com/ https://vuldb.com/?ctiid.306794 https://vuldb.com/?id.306794 https://vuldb.com/?submit.561746
https://nvd.nist.gov/vuln/detail/CVE-2025-4164	**7,3**	PHPGurukul Employee Record Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.3	https://github.com/ideal-valli/myCVE/issues/2 https://phpgurukul.com/ https://vuldb.com/?ctiid.306696 https://vuldb.com/?id.306696 https://vuldb.com/?submit.561140
https://nvd.nist.gov/vuln/detail/CVE-2025-4153	**7,3**	PHPGurukul Park Ticketing Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 2.0	https://github.com/y77-88/myCVE/issues/2 https://phpgurukul.com/ https://vuldb.com/?ctiid.306685 https://vuldb.com/?id.306685 https://vuldb.com/?submit.560809

https://nvd.nist.gov/vuln/detail/CVE-2025-4152	**7,3**	PHPGurukul Online Birth Certificate System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/faithhard/cve/issues/2 https://phpgurukul.com/ https://vuldb.com/?ctiid.306684 https://vuldb.com/?id.306684 https://vuldb.com/?submit.560808
https://nvd.nist.gov/vuln/detail/CVE-2025-4151	**7,3**	PHPGurukul Curfew e-Pass Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 1.0	https://github.com/faithhard/cve/issues/1 https://phpgurukul.com/ https://vuldb.com/?ctiid.306683 https://vuldb.com/?id.306683 https://vuldb.com/?submit.560806
https://nvd.nist.gov/vuln/detail/CVE-2025-4112	**7,3**	PHPGurukul Student Record System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version 3.2	https://github.com/bleakTS/myCVE/issues/3 https://phpgurukul.com/ https://vuldb.com/?ctiid.306592 https://vuldb.com/?id.306592 https://vuldb.com/?submit.560701

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2024-38475 Apache HTTP Server Improper Escaping of Output Vulnerability ▪ CVE-2023-44221 SonicWall SMA100 Appliances OS Command Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2025/05/01/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Releases Two Industrial Control Systems Advisories	▪ ICSA-25-121-01 KUNBUS GmbH Revolution Pi ▪ ICSMA-25-121-01 MicroDicom DICOM Viewer	https://www.cisa.gov/news-events/alerts/2025/05/01/cisa-releases-two-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
Microsoft makes all new accounts passwordless by default	https://www.bleepingcomputer.com/news/microsoft/microsoft-makes-all-new-accounts-passwordless-by-default/
Scammers Use Spain-Portugal Blackout for TAP Air Refund Phishing Scam	https://hackread.com/spain-portugal-blackout-tap-air-refund-phishing-scam/
Canadian electric utility Nova Scotia Power and parent company Emera suffered a cyberattack	https://securityaffairs.com/177281/hacking/canadian-electric-utility-nova-scotia-power-and-parent-company-emera-suffered-a-cyberattack.html
Mystery Box Scams Deployed to Steal Credit Card Data	https://www.infosecurity-magazine.com/news/mystery-box-scams-credit-card-data/
SK Telecom Offers Free SIM Replacements After Malware Breach Impacts USIM Data	https://dailysecurityreview.com/security-spotlight/sk-telecom-offers-free-sim-replacements-after-malware-breach-impacts-usim-data/
#Infosec2025: How Advances in Quantum Computing Could Reshape Cybersecurity	https://www.infosecurity-magazine.com/news/infosec2025-quantum-reshape/
Claude Chatbot Used for Automated Political Messaging	https://www.infosecurity-magazine.com/news/claude-chatbot-political-messaging/
Trellix DLP Endpoint Complete prevents data leaks in Windows and macOS	https://www.helpnetsecurity.com/2025/04/30/trellix-dlp-endpoint-complete/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
MTN Ghana Data Breach Impacts 5,700 Customers, Investigation Underway	https://dailysecurityreview.com/security-spotlight/mtn-ghana-data-breach-impacts-5700-customers-investigation-underway/
LummaStealer's FakeCAPTCHA Steals Browser Credentials Via Weaponized Microsoft Word Files	https://cybersecuritynews.com/lummastealers-fakecaptcha-steals-browser-credentials/
Harrods Store Hit by Cyber Attack Following Marks & Spencer and Co-op	https://cybersecuritynews.com/harrods-store-hit-by-cyber-attack/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
U.S. CISA adds SonicWall SMA100 and Apache HTTP Server flaws to its Known Exploited Vulnerabilities catalog	https://securityaffairs.com/177301/hacking/u-s-cisa-adds-sonicwall-sma100-and-apache-http-server-flaws-to-its-known-exploited-vulnerabilities-catalog.html
Ticket Resale Platform TicketToCash Left 200GB of User Data Exposed	https://hackread.com/ticket-resale-platform-tickettocash-exposed-user-data/
Researchers Demonstrate How MCP Prompt Injection Can Be Used for Both Attack and Defense	https://thehackernews.com/2025/04/experts-uncover-critical-mcp-and-a2a.html
Apple 'AirBorne' flaws can lead to zero-click AirPlay RCE attacks	https://www.bleepingcomputer.com/news/security/apple-airborne-flaws-can-lead-to-zero-click-airplay-rce-attacks/
Oracle VirtualBox Vulnerability Exposes Systems to Privilege Escalation Attacks	https://cybersecuritynews.com/virtualbox-vulnerability-privilege-escalation-attacks/
New WordPress Malware as Anti-Malware Plugin Take Full Control of Website	https://cybersecuritynews.com/new-wordpress-malware-as-anti-malware-plugin/
CISA Warns of SonicWall SMA100 OS Command Injection Vulnerability Exploited in Wild	https://cybersecuritynews.com/sonicwall-sma100-os-command-injection/
U.S. CISA adds SAP NetWeaver flaw to its Known Exploited Vulnerabilities catalog	https://securityaffairs.com/177218/hacking/u-s-cisa-adds-sap-netweaver-flaw-to-its-known-exploited-vulnerabilities-catalog.html
CISA Flags Broadcom, CommVault, and Active! Mail Vulnerabilities as Actively Exploited	https://dailysecurityreview.com/security-spotlight/cisa-flags-broadcom-commvault-and-active-mail-vulnerabilities-as-actively-exploited/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Microsoft: Windows 11 24H2 updates fail with 0x80240069 errors	https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-11-24h2-updates-fail-with-0x80240069-errors/
Chrome 136, Firefox 138 Patch High-Severity Vulnerabilities	https://www.securityweek.com/chrome-136-firefox-138-patch-high-severity-vulnerabilities/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Malicious PyPI packages abuse Gmail, websockets to hijack systems	https://www.bleepingcomputer.com/news/security/malicious-pypi-packages-abuse-gmail-websockets-to-hijack-systems/
Chinese Hackers Abuse IPv6 SLAAC for AitM Attacks via Spellbinder Lateral Movement Tool	https://thehackernews.com/2025/04/chinese-hackers-abuse-ipv6-slaac-for.html
Pro-Russia hacktivist group NoName057(16) is targeting Dutch organizations	https://securityaffairs.com/177312/hacktivism/pro-russia-hacktivist-group-noname05716-is-targeting-dutch-organizations.html
New Powerful Nullpoint-Stealer With Extensive Capabilities Hosted on GitHub	https://cybersecuritynews.com/powerful-nullpoint-stealer/
RansomHub Refines Extortion Strategy as RaaS Market Fractures	https://www.infosecurity-magazine.com/news/ransomhub-refines-extortion/
npm Malware Targets Crypto Wallets, MongoDB; Code Points to Turkey	https://hackread.com/npm-malware-crypto-wallets-mongodb-turkey-code/
FBI shared a list of phishing domains associated with the LabHost PhaaS platform	https://securityaffairs.com/177293/cyber-crime/fbi-shared-a-list-of-phishing-domains-associated-with-the-labhost-phaas-platform.html

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/