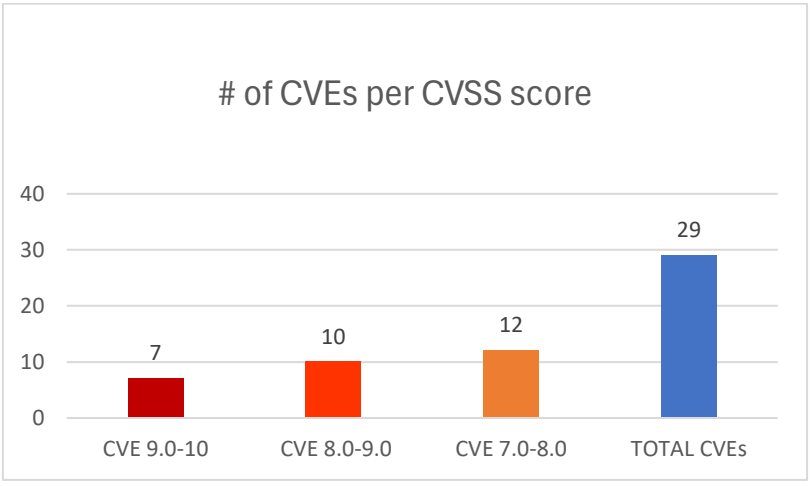
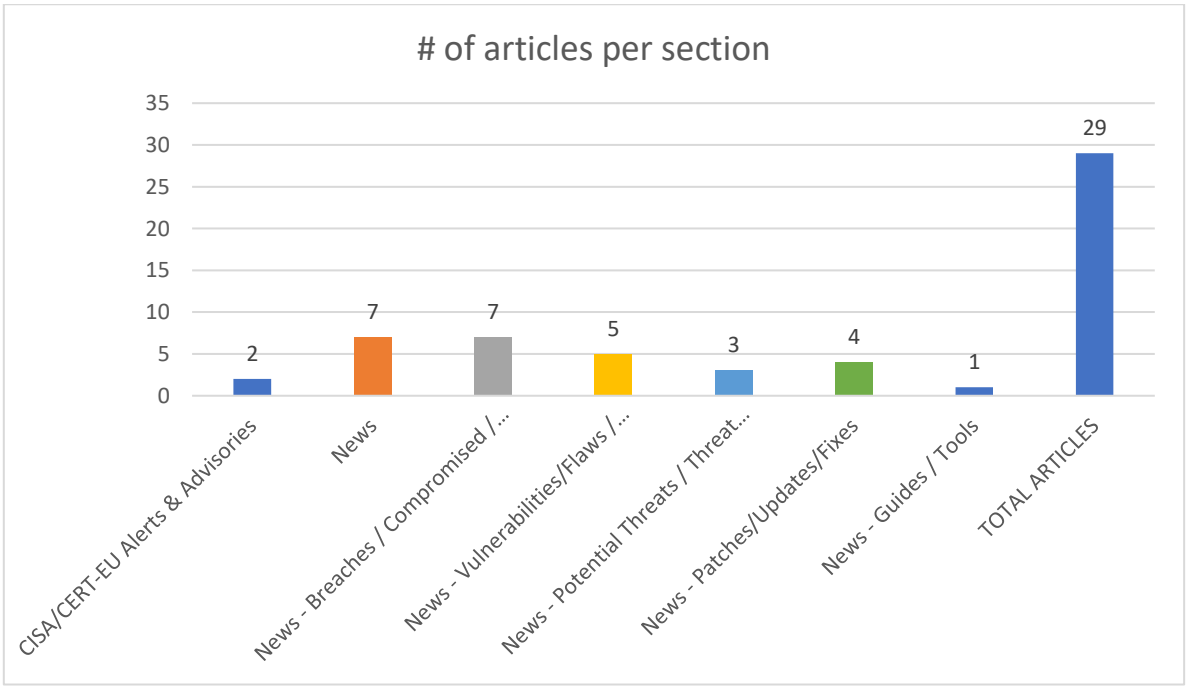
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 02/07/2025 - 04/07/2025





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-2025-20309	10,0	Cisco Unified Communications Manager (Unified CM)	Use of Hard-coded Credentials		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssh-m4UBdpE7
https://nvd.nist.gov/vuln/detail/CVE-2024-13786	9,8	The education theme for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 3.6.10	https://themeforest.net/item/education-center-training-courses-wordpress-theme/10652918#item-description__change-log https://www.wordfence.com/threat-intel/vulnerabilities/id/d0b27bc8-617a-4f98-954f-e49f87dca311?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-5746	9,8	The Drag and Drop Multiple File Upload (Pro) - WooCommerce plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 1.7.1	https://www.codedropz.com/woocommerce-drag-drop-multiple-file-upload/ https://www.wordfence.com/threat-intel/vulnerabilities/id/3c1f625e-4456-45e4-8a7f-809b22edb66b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-45813	9,8	ENENSYS IPGuard	Use of Hard-coded Credentials	v2 2.10.0	https://github.com/shiky8/my--cve-vulnerability-research/tree/main/CVE-2025-45813 https://www.enensys.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-45814	9,8	query.fcgi endpoint of NS3000	Missing Authentication for Critical Function	v8.1.1.125110 , v7.2.8.124852 , and v7.x and NS2000 v7.02.08	https://github.com/shiky8/my--cve-vulnerability-research/tree/main/CVE-2025-45814 https://novelsat.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6513	9,3	BRAIN2	Password in Configuration File		https://www.bizerba.com/downloads/global/information-security/2025/bizerba-sa-2025-0003.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-23968	9,1	WPCenter AiBud WP	Unrestricted Upload of File with Dangerous Type	AiBud WP: from n/a through 1.8.5	https://patchstack.com/database/wordpress/plugin/aibuddy-openai-chatgpt/vulnerability/wordpress-aibud-wp-plugin-1-8-5-arbitrary-file-upload-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-6459	8,8	The Ads Pro Plugin - Multi-Purpose WordPress Advertising Manager plugin for WordPress	Cross-Site Request Forgery (CSRF)	all versions up to, and including, 4.89	https://codecanyon.net/item/ads-pro-plugin-multi-purpose-wordpress-advertising-manager/10275010 https://www.wordfence.com/threat-intel/vulnerabilities/id/22fa8290-ebab-4fa4-bcba-0053c3b79f76?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-49713	8,8	Microsoft Edge (Chromium-based)	Access of Resource Using Incompatible Type ('Type Confusion')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49713
https://nvd.nist.gov/vuln/detail/CVE-2025-49126	8,8	Visionatrix	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	In versions 1.5.0 to before 2.5.1	https://github.com/Visionatrix/Visionatrix/commit/63aafe6e4d1bffe4bf69e73b6fdfc65c71a8f5b8 https://github.com/Visionatrix/Visionatrix/security/advisories/GHSA-w36r-9jvx-q48v
https://nvd.nist.gov/vuln/detail/CVE-2025-5953	8,8	The WP Human Resource Management plugin for WordPress	Missing Authorization	versions 2.0.0 through 2.2.17	https://plugins.trac.wordpress.org/browser/hrm/tags/2.2.17/class/employee.php#L543 https://plugins.trac.wordpress.org/browser/hrm/tags/2.2.17/class/employee.php#L591 https://plugins.trac.wordpress.org/browser/hrm/tags/2.2.17/class/employee.php#L89 https://wordpress.org/plugins/hrm/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/3ba33a18-429f-4a3e-b018-bdfbbe6e8482?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-6926	8,8	Wikimedia Foundation Mediawiki	Improper Authentication	from 1.39.X before 1.39.13, from 1.42.X before 1.42.7, from 1.43.X before 1.43.2	https://gerrit.wikimedia.org/r/c/mediawiki/core/+/1165117 https://phabricator.wikimedia.org/T389010

https://nvd.nist.gov/vuln/detail/CVE-2025-2932	8,8	The JKDEVKIT plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 1.9.4	http://example.com/wp-content/plugins/jkdev-kit/inc/modules/fonts_manager.php#L1710 https://www.wordfence.com/threat-intel/vulnerabilities/id/68679ff9-48a8-4146-a37f-5f844dc86c92?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53369	8,6	Short Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	version 4.0.0	https://github.com/StarCitizenTools/mediawiki-extensions-ShortDescription/commit/bc4fdbaeb1dff127fb6d08c0d385b64aa128c8f8 https://github.com/StarCitizenTools/mediawiki-extensions-ShortDescription/security/advisories/GHSA-p85q-mww9-gwqf
https://nvd.nist.gov/vuln/detail/CVE-2025-4946	8,1	The Vikinger theme for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 1.9.32	https://themeforest.net/item/vikinger-buddypress-and-gamipress-social-community/28612259 https://www.wordfence.com/threat-intel/vulnerabilities/id/22d8f1db-1b7e-4b68-a381-01f51dd34b2b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-50263	8,1	Tenda AC6	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	v15.03.05.16	https://github.com/faqiadegege/IoTVuln/blob/main/tendaAC6_SetStaticRouteCfg_list_overflow/detail.md
https://nvd.nist.gov/vuln/detail/CVE-2025-6238	8,0	The AI Engine plugin for WordPress	URL Redirection to Untrusted Site ('Open Redirect')	version 2.8.4	https://plugins.trac.wordpress.org/browser/ai-engine/tags/2.8.4/labs/oauth.php https://plugins.trac.wordpress.org/changeset/3321384/ai-engine/trunk/labs/mcp.php https://plugins.trac.wordpress.org/changeset/3321384/ai-engine/trunk/labs/oauth.php https://www.wordfence.com/threat-intel/vulnerabilities/id/1edc84fd-8cb5-4899-9444-1b6ae3144917?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-6464	7,5	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 1.44.2	https://plugins.trac.wordpress.org/browser/forminator/trunk/library/model/class-form-entry-model.php#L1249 https://plugins.trac.wordpress.org/browser/forminator/trunk/library/model/class-form-entry-model.php#L1263 https://plugins.trac.wordpress.org/changeset?old_path=%2Fforminator&old=3319860&new_path=%2Fforminator&new=3319860&sfp_email=&sfph_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/6707aa4c-c652-42c0-bdb9-00be984e7271?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-6814	7,5	The Booking X plugin for WordPress	Missing Authorization	versions 1.0 to 1.1.2	https://plugins.trac.wordpress.org/browser/bookingx/tags/1.1.2/admin/class-bookingx-admin.php#L784 https://plugins.trac.wordpress.org/browser/bookingx/tags/1.1.2/includes/class-bookingx.php#L322 https://wordpress.org/plugins/booking-x/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/6a30d572-e086-4b83-8cb7-4cef9a3253bd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-6783	7,5	The GoZen Forms plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 1.1.5	https://wordpress.org/plugins/gozen-forms/ https://www.wordfence.com/threat-intel/vulnerabilities/id/784998a7-550d-4299-9995-af01e5ee1d21?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-49826	7,5	Next.js	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	From versions 15.0.4-canary.51 to before 15.1.8	https://github.com/vercel/next.js/commit/a15b974ed707d63ad4da5b74c1441f5b7b120e93 https://github.com/vercel/next.js/releases/tag/v15.1.8 https://github.com/vercel/next.js/security/advisories/GHSA-67rr-84xm-4c7r https://vercel.com/changelog/cve-2025-49826

https://nvd.nist.gov/vuln/detail/CVE-2025-6072	7,5	ABB RMC-100, ABB RMC-100 LITE	Stack-based Buffer Overflow	RMC-100: from 2105457-043 through 2105457-045; RMC-100 LITE: from 2106229-015 through 2106229-016	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108471A3623&LanguageCode=en&DocumentPartId=PDF&Action=Launch
https://nvd.nist.gov/vuln/detail/CVE-2025-27456	7,5	The SMB server's login mechanism	Improper Restriction of Excessive Authentication Attempts		https://sick.com/psirt https://sick.com/psirt https://www.cisa.gov/resources-tools/resources/ics-recommended-practices https://www.endress.com https://www.first.org/cvss/calculator/3.1 https://www.sick.com/.well-known/csaf/white/2025/sca-2025-0008.json https://www.sick.com/.well-known/csaf/white/2025/sca-2025-0008.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-1710	7,5	The maxView Storage Manager	Improper Restriction of Excessive Authentication Attempts		https://sick.com/psirt https://sick.com/psirt https://www.cisa.gov/resources-tools/resources/ics-recommended-practices https://www.endress.com https://www.first.org/cvss/calculator/3.1 https://www.sick.com/.well-known/csaf/white/2025/sca-2025-0008.json https://www.sick.com/.well-known/csaf/white/2025/sca-2025-0008.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-27387	7,4	OPPO Clone Phone	Exposure of Sensitive Information to an Unauthorized Actor		https://security.oppo.com/en/noticeDetail?notice_only_key=NOTICE-1937080145974403072https://
https://nvd.nist.gov/vuln/detail/CVE-2024-9017	7,2	The PeepSo Core: Groups plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	in all versions up to, and including, 6.4.6.0	https://www.peepso.com/changelog/ https://www.wordfence.com/threat-intel/vulnerabilities/id/32ac79f4-ada7-4c14-8675-53f8375912d8?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-6586	7,2	The Download Plugin plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 2.2.8	https://plugins.trac.wordpress.org/browser/download-plugin/tags/2.2.8/app/Plugins/Dpwapuploader.php#L300 https://www.wordfence.com/threat-intel/vulnerabilities/id/37734c25-cce3-41fb-babf-714ba7a4bced?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-5322	7,2	The VikRentCar Car Rental Management System plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 1.4.3	https://plugins.trac.wordpress.org/browser/vikrentcar/tags/1.4.3/admin/controller.php#L1418 https://plugins.trac.wordpress.org/browser/vikrentcar/tags/1.4.3/admin/controller.php#L1698 https://plugins.trac.wordpress.org/changeset/3317493/ https://www.wordfence.com/threat-intel/vulnerabilities/id/5f837ba2-64a2-4d8e-8212-b646cb94b0d7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-5961	7,2	The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 0.9.116	https://github.com/d0n601/CVE-2025-5961 https://plugins.trac.wordpress.org/browser/wpvivid-backuprestore/trunk/includes/class-wpvivid-export-import.php#L2210 https://plugins.trac.wordpress.org/browser/wpvivid-backuprestore/trunk/includes/class-wpvivid-export-import.php#L2235 https://plugins.trac.wordpress.org/browser/wpvivid-backuprestore/trunk/includes/class-wpvivid-export-import.php#L2246 https://plugins.trac.wordpress.org/changeset/3320877/ https://ryankozak.com/posts/cve-2025-5961/ https://www.wordfence.com/threat-intel/vulnerabilities/id/d8ceb4a1-9354-4ed3-9a8f-45ba2057a810?source=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-6554 Google Chromium V8 Type Confusion Vulnerability	https://www.cisa.gov/news-events/alerts/2025/07/02/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Four Industrial Control Systems Advisories	▪ ICSA-25-184-01 Hitachi Energy Relion 670/650 and SAM600-IO Series ▪ ICSA-25-184-02 Hitachi Energy MicroSCADA X SYS600 ▪ ICSA-25-184-03 Mitsubishi Electric MELSOFT Update Manager ▪ ICSA-25-184-04 Mitsubishi Electric MELSEC iQ-F Series	https://www.cisa.gov/news-events/alerts/2025/07/03/cisa-releases-four-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
Google Ordered to Pay $314M for Misusing Android Users' Cellular Data Without Permission	https://thehackernews.com/2025/07/google-ordered-to-pay-314m-for-misusing.html
EU Launches Plan to Implement Quantum-Secure Infrastructure	https://www.infosecurity-magazine.com/news/eu-plan-quantum-secure/
Africa's cybersecurity crisis and the push to mobilizing communities to safeguard a digital future	https://www.helpnetsecurity.com/2025/07/04/africa-cybersecurity-crisis/
CVE Program Launches Two New Forums to Enhance CVE Utilization	https://www.infosecurity-magazine.com/news/cve-program-new-user-researcher/
China-linked group Houken hit French organizations using zero-days	https://securityaffairs.com/179602/apt/china-linked-group-houken-hit-french-organizations-using-zero-days.html
Massive Android Fraud Operations Uncovered: IconAds, Kaleidoscope, SMS Malware, NFC Scams	https://thehackernews.com/2025/07/mobile-security-alert-352-iconads-fraud.html
Threat Intelligence Executive Report – Volume 2025, Number 3	https://news.sophos.com/en-us/2025/07/03/threat-intelligence-executive-report-volume-2025-number-3/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Cybercriminals Target Brazil: 248,725 Exposed in CIEE One Data Breach	https://securityaffairs.com/179609/data-breach/cybercriminals-target-brazil-248725-exposed-in-ciee-one-data-breach.html
IdeaLab confirms data stolen in ransomware attack last year	https://www.bleepingcomputer.com/news/security/idealab-confirms-data-stolen-in-ransomware-attack-last-year/
Android SMS Stealer Infects 100,000 Devices in Uzbekistan	https://www.infosecurity-magazine.com/news/android-sms-stealer-100000/
Kelly Benefits data breach has impacted 550,000 people, and the situation continues to worsen as the investigation progresses	https://securityaffairs.com/179583/uncategorized/the-kelly-benefits-data-breach-has-impacted-550000-people-and-the-situation-continues-to-worsen-as-the-investigation-progresses.html
A sophisticated cyberattack hit the International Criminal Court	https://securityaffairs.com/179532/hacking/a-sophisticated-cyberattack-hit-the-international-criminal-court.html
Virginia county says April ransomware attack exposed employee SSNs	https://therecord.media/virginia-county-says-ransomware-attack-exposed-ssns?&web_view=true
Columbia University breach attributed to politically motivated hacker	https://scmagazine.com/brief/columbia-university-breach-attributed-to-politically-motivated-hacker

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
WordPress Plugin Flaw Exposes 600,000 Sites to File Deletion	https://www.infosecurity-magazine.com/news/wordpress-plugin-flaw-sites-file/
Privilege Escalation Flaw Found in Azure Machine Learning Service	https://www.infosecurity-magazine.com/news/privilege-escalation-flaw-azure-ml/
Forminator plugin flaw exposes WordPress sites to takeover attacks	https://www.bleepingcomputer.com/news/security/forminator-plugin-flaw-exposes-wordpress-sites-to-takeover-attacks/
Apache Tomcat and Camel Vulnerabilities Actively Exploited in The Wild	https://cybersecuritynews.com/apache-tomcat-and-camel-vulnerabilities/
Microsoft: DNS issue blocks delivery of Exchange Online OTP codes	https://www.bleepingcomputer.com/news/microsoft/microsoft-links-dns-issue-to-exchange-online-otp-delivery-failures/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Grafana releases critical security update for Image Renderer plugin	https://www.bleepingcomputer.com/news/security/grafana-releases-critical-security-update-for-image-renderer-plugin/
Cisco fixes maximum-severity flaw in enterprise unified comms platform (CVE-2025-20309)	https://www.helpnetsecurity.com/2025/07/03/cisco-fixes-maximum-severity-flaw-in-enterprise-unified-comms-platform-cve-2025-20309/
Microsoft fixes 'Print to PDF' feature broken by Windows update	https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-print-to-pdf-feature-broken-by-windows-update/
Linux Users Urged to Patch Critical Sudo CVE	https://www.infosecurity-magazine.com/news/linux-users-urged-to-patch/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Over 40 Malicious Firefox Extensions Target Cryptocurrency Wallets, Stealing User Assets	https://thehackernews.com/2025/07/over-40-malicious-firefox-extensions.html
Citrix warns of login issues after NetScaler auth bypass patch	https://www.bleepingcomputer.com/news/security/citrix-warns-of-login-issues-after-netscaler-auth-bypass-patch/
Automation and Vulnerability Exploitation Drive Mass Ransomware Breaches	https://www.infosecurity-magazine.com/news/automation-vulnerability/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-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/