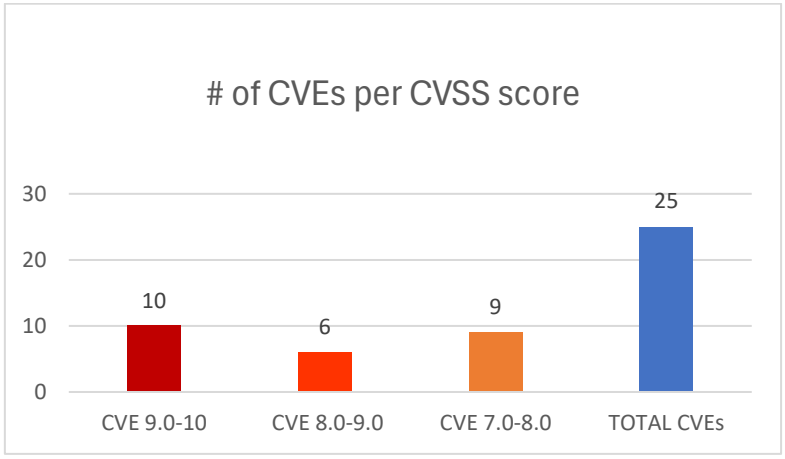
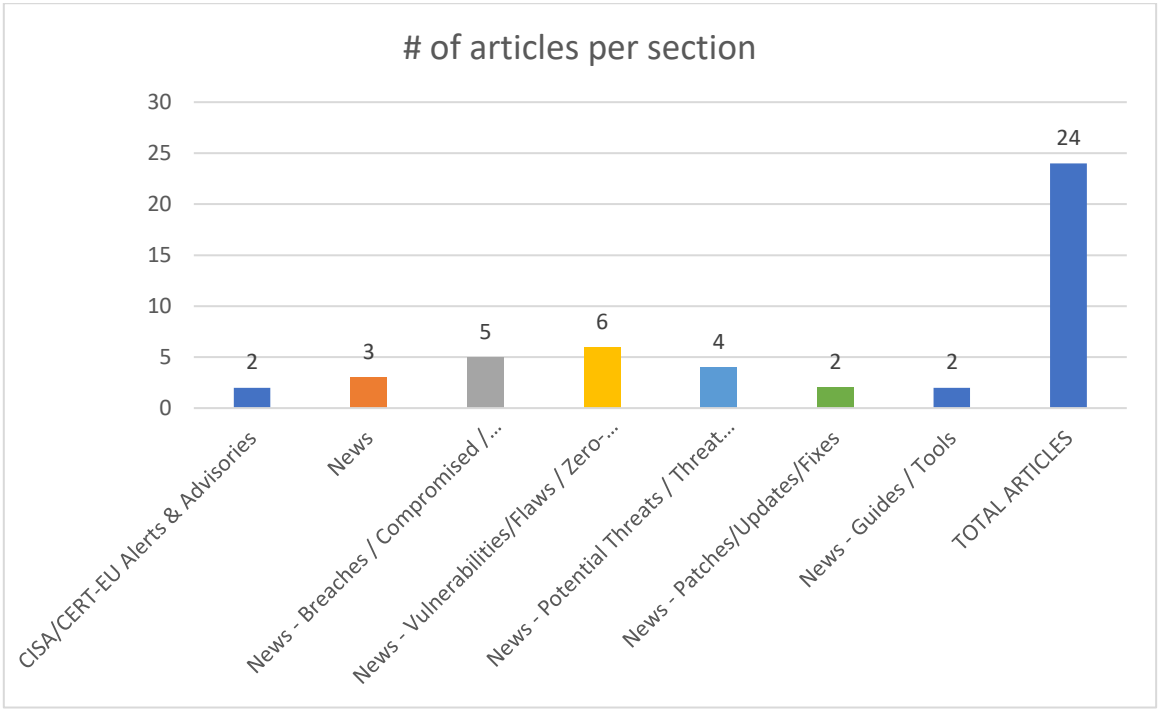
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 19/07/2025 - 22/07/2025





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-2012-10020	9,8	The FoxyPress plugin for WordPress	Unrestricted Upload of File with Dangerous Type	versions up to, and including, 0.4.2.1	https://packetstormsecurity.com/files/113576/ https://plugins.trac.wordpress.org/changeset/555071 https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/unix/webapp/wp_foxypress_upload.rb https://web.archive.org/web/20210120060045/https%3A//www.securityfocus.com/bid/53805/info https://www.wordfence.com/threat-intel/vulnerabilities/id/8fbc88da-8944-433c-b94d-9604ffe13d8a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2015-10137	9,8	The Website Contact Form With File Upload plugin for WordPress	Unrestricted Upload of File with Dangerous Type	versions up to, and including, 1.3.4	https://packetstormsecurity.com/files/131413/ https://packetstormsecurity.com/files/131514/ https://plugins.trac.wordpress.org/browser/website-contact-form-with-file-upload/trunk/readme.txt https://plugins.trac.wordpress.org/browser/website-contact-form-with-file-upload/trunk/readme.txt#L147 https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-n-media-website-contact-form-with-file-upload-arbitrary-file-upload-1-3-4/ https://www.homelab.it/index.php/2015/04/12/wordpress-n-media-website-contact-form-shell-upload/ https://www.wordfence.com/threat-intel/vulnerabilities/id/8395e0c4-3feb-4551-9f2f-7b80cd187eca?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7343	9,8	The SFT developed by Digiwin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://www.digiwin.com/tw/news/3568.html https://www.twcert.org.tw/en/cp-139-10271-25ea9-2.html https://www.twcert.org.tw/tw/cp-132-10270-83d95-1.html
https://nvd.nist.gov/vuln/detail/CVE-2015-10138	9,8	The Work The Flow File Upload plugin for WordPress	Unrestricted Upload of File with Dangerous Type	versions up to, and including, 2.5.2.	https://packetstormsecurity.com/files/131294/ https://packetstormsecurity.com/files/131512/ https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=1127456%40work-the-flow-file-upload&new=1127456%40work-the-flow-file-upload&sfp_email=&sfph_mail=

					https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=1127457%40work-the-flow-file-upload&new=1127457%40work-the-flow-file-upload&sfp_email=&sfph_mail= https://wpscan.com/vulnerability/a49a81a9-3d4b-4c8d-b719-fc513aceecc6 https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-work-the-flow-file-upload-arbitrary-file-upload-2-5-2/ https://www.homelab.it/index.php/2015/04/04/wordpress-work-the-flow-file-upload-vulnerability/ https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_worktheflow_upload/ https://www.wordfence.com/threat-intel/vulnerabilities/id/eb271cc8-01ec-45eb-9d6f-efc55c7c3923?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2015-10135	9,8	The WPshop 2 – E-Commerce plugin for WordPress	Unrestricted Upload of File with Dangerous Type	versions before 1.3.9.6	https://g0blin.co.uk/g0blin-00036/ https://github.com/espreto/wpsploit/blob/master/modules/exploits/unix/webapp/wp_wpshop_ecommerce_file_upload.rb https://plugins.trac.wordpress.org/changeset/1103406 https://wordpress.org/plugins/wpshop/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/32e8224d-a653-48d7-a3f4-338fc0c1dc77?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2012-10019	9,8	The Front End Editor plugin for WordPress	Unrestricted Upload of File with Dangerous Type	in versions before 2.3.	https://packetstormsecurity.com/files/132303/ https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=600233%40front-end-editor&old=569105%40front-end-editor&sfp_email=&sfph_mail= https://web.archive.org/web/20120712205339/https%3A//www.opensyscom.fr/Actualites/wordpress-plugins-front-end-editor-arbitrary-file-upload-vulnerability.html https://www.cybersecurity-help.cz/vdb/SB2012070701 https://www.wordfence.com/threat-intel/vulnerabilities/id/f271c2e7-9d58-4dea-95d3-3ffc4ec7c3b2?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7697	9,8	The Integration for Google Sheets and Contact Form 7,	Deserialization of Untrusted Data	all versions up to, and including, 1.1.1	https://plugins.trac.wordpress.org/browser/integration-for-contact-form-7-and-google-sheets/tags/1.1.1/integration-for-contact-form-7-and-google-sheets.php#L923 https://plugins.trac.wordpress.org/changeset/3329005/

		WPForms, Elementor, Ninja Forms plugin for WordPress			https://wordpress.org/plugins/integration-for-contact-form-7-and-google-sheets/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/a0146f17-35bd-45cf-b9c6-c4fce688efc2?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7696	9,8	The Integration for Pipedrive and Contact Form 7, WPForms, Elementor, Ninja Forms plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 1.2.3	https://plugins.trac.wordpress.org/browser/integration-for-contact-form-7-and-pipedrive/tags/1.2.3/integration-for-contact-form-7-and-pipedrive.php#L953 https://plugins.trac.wordpress.org/changeset/3329002/ https://wordpress.org/plugins/integration-for-contact-form-7-and-pipedrive/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/6980112b-a555-47a4-b2d7-f0187d52fc63?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7916	9,8	WinMatrix3 developed by Simopro Technology	Deserialization of Untrusted Data		https://www.twcert.org.tw/en/cp-139-10257-e88f3-2.html https://www.twcert.org.tw/tw/cp-132-10256-14d55-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-53770	9,8	Microsoft SharePoint Server	Deserialization of Untrusted Data	cpe:2.3:a:microsoft:share-point_server:*:*:*:*:subscription:*:*:* Show Matching CPE(s) Up to (excluding) 16.0.18526.20508 cpe:2.3:a:microsoft:share-point_server:2016:*:*:*:enterprise:*:*:* Show Matching CPE(s)	https://arstechnica.com/security/2025/07/sharepoint-vulnerability-with-9-8-severity-rating-is-under-exploit-across-the-globe/ https://github.com/kaizensecurity/CVE-2025-53770 Exploit https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/ Mitigation Vendor Advisory https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770 Vendor Advisory https://news.ycombinator.com/item?id=44629710 https://research.eye.security/sharepoint-under-siege/ Exploit Mitigation Third Party Advisory https://therecord.media/microsoft-sharepoint-zero-day-vulnerability-exploited-globally Press/Media Coverage https://www.bleepingcomputer.com/news/microsoft/microsoft-sharepoint-zero-day-exploited-in-rce-attacks-no-patch-available/ Press/Media Coverage https://www.cisa.gov/news-events/alerts/2025/07/20/microsoft-releases-guidance-exploitation-sharepoint-vulnerability-cve-2025-53770 Mailing List Third Party Advisory US Government Resource

				cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*:* Show Matching CPE(s)	https://www.darkreading.com/remote-workforce/microsoft-rushes-emergency-fix-exploited-sharepoint-toolshell-flaw https://www.forbes.com/sites/daveywinder/2025/07/20/microsoft-confirms-ongoing-mass-sharepoint-attack---no-patch-available/ Press/Media Coverage https://x.com/Shadowserver/status/1946900837306868163
https://nvd.nist.gov/vuln/detail/CVE-2025-7945	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	DIR-513 up to 20190831	https://github.com/LYN1ng/D-linkdir513/blob/main/Dlink_DIR-513_Buffer_Overflow_Vulnerability.md
https://nvd.nist.gov/vuln/detail/CVE-2025-7344	8,8	The EAI developed by Digiwin	Incorrect Use of Privileged APIs		https://www.digiwin.com/tw/news/3567.html https://www.twcert.org.tw/en/cp-139-10273-ce2ed-2.html https://www.twcert.org.tw/tw/cp-132-10272-5b691-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-7912	8,8	TOTOLINK	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	T6 4.1.5cu.748_B20211015	https://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/6.md https://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/6.md#poc https://vuldb.com/?ctiid.317027 https://vuldb.com/?id.317027 https://vuldb.com/?submit.618655 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-7914	8,8	Tenda	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	AC6 15.03.06.50	https://github.com/gaochen61/IoTVuln/blob/main/Tenda_AC6_V15.03.06.50/setparentcontrolinfo.md https://vuldb.com/?ctiid.317029 https://vuldb.com/?id.317029 https://vuldb.com/?submit.618859 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-6585	8,1	The WP JobHunt plugin for WordPress	Improper Input Validation	all versions up to, and including, 7.2	https://themeforest.net/item/jobcareer-job-board-responsive-wordpress-theme/14221636 https://www.wordfence.com/threat-intel/vulnerabilities/id/afb3e0e0-68c7-43f6-981f-59c3f3507429?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-7645	8,1	The Extensions For CF7	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 3.2.8	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3330857%40extensions-for-cf7&new=3330857%40extensions-for-cf7&sfp_email=&sfph_mail=
https://nvd.nist.gov/vuln/detail/CVE-2025-4129	7,5	PAVO Inc	Authorization Bypass Through User-Controlled Key	PAVO Pay: before 13.05.2025	https://www.usom.gov.tr/bildirim/tr-25-0166
https://nvd.nist.gov/vuln/detail/CVE-2025-1469	7,5	Turtek Software Eyotek	Authorization Bypass Through User-Controlled Key	Eyotek: before 11.03.2025	https://www.usom.gov.tr/bildirim/tr-25-0163
https://nvd.nist.gov/vuln/detail/CVE-2015-10134	7,5	The Simple Backup plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	versions up to, and including, 2.7.10	https://packetstormsecurity.com/files/131919/ https://www.wordfence.com/threat-intel/vulnerabilities/id/29482b70-0ff2-4bb1-9d41-9cffb83b5ad0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7933	7,3	Campcodes Sales and Inventory System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/zhaodaojie/cve/issues/5 https://vuldb.com/?ctiid.317062 https://vuldb.com/?id.317062 https://vuldb.com/?submit.618952 https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-7931	7,3	Church Donation System	Improper Access Control	1.0	https://code-projects.org/ https://github.com/n0name-yang/myCVE/issues/16 https://vuldb.com/?ctiid.317060 https://vuldb.com/?id.317060 https://vuldb.com/?submit.618946
https://nvd.nist.gov/vuln/detail/CVE-2025-7915	7,3	Chanjet CRM	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/qiantx/cve/blob/main/cve4.md https://vuldb.com/?ctiid.317030 https://vuldb.com/?id.317030 https://vuldb.com/?submit.618873

https://nvd.nist.gov/vuln/detail/CVE-2025-7897	7,3	harry0703 MoneyPrinterTurbo	Improper Authentication	up to 1.2.6	https://vuldb.com/?ctiid.317012 https://vuldb.com/?id.317012 https://vuldb.com/?submit.609040
https://nvd.nist.gov/vuln/detail/CVE-2025-7886	7,3	pmTicket Project-Management-Software	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to 2ef379da2075f4761a2c9029cf91d073474e7486	https://asciinema.org/a/3wu3WGpnrnMc2GDvSyLUqqHUF https://vuldb.com/?ctiid.317001 https://vuldb.com/?id.317001 https://vuldb.com/?submit.614534
https://nvd.nist.gov/vuln/detail/CVE-2015-10133	7,2	The Subscribe to Comments for WordPress	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion)	versions up to, and including, 2.1.2	https://advisories.dxw.com/advisories/admin-only-local-file-inclusion-and-arbitrary-code-execution-in-subscribe-to-comments-2-1-2/ https://packetstormsecurity.com/files/132694/ https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=1198281%40subscribe-to-comments&new=1198281%40subscribe-to-comments&sfp_email=&sfph_mail= https://seclists.org/fulldisclosure/2015/Jul/71 https://www.wordfence.com/threat-intel/vulnerabilities/id/f92784a7-f2b3-47f8-b03f-4e234b57e40a?source=cve

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability, CVE-2025-53770 “ToolShell,” to Catalog	▪ CVE-2025-53770: Microsoft SharePoint Server Remote Code Execution Vulnerability	https://www.cisa.gov/news-events/alerts/2025/07/20/cisa-adds-one-known-exploited-vulnerability-cve-2025-53770-toolshell-catalog
Microsoft Releases Guidance on Exploitation of SharePoint Vulnerability (CVE-2025-53770)		https://www.cisa.gov/news-events/alerts/2025/07/20/microsoft-releases-guidance-exploitation-sharepoint-vulnerability-cve-2025-53770

News

Σύντομη περιγραφή / Τίτλος	URL
Hackers Exploit SharePoint Zero-Day Since July 7 to Steal Keys, Maintain Persistent Access	https://thehackernews.com/2025/07/hackers-exploit-sharepoint-zero-day.html
CISA Issues Advisories on Critical ICS Vulnerabilities Across Multiple Sectors	https://www.infosecurity-magazine.com/news/cisa-issues-advisories-ics-vulns/
Europol Sting Leaves Russian Cybercrime's 'NoName057(16)' Group Fractured	https://www.darkreading.com/threat-intelligence/europol-sting-russian-cybercrime-noname05716

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
World Leaks Claims Dell Data Breach, Leaks 1.3 TB of Files	https://hackread.com/world-leaks-dell-data-breach-leaks-1-3-tb-of-files/
Dell confirms breach of test lab platform by World Leaks extortion group	https://www.bleepingcomputer.com/news/security/dell-confirms-breach-of-test-lab-platform-by-world-leaks-extortion-group/
Boston clinic notifies 185,000+ people of data breach that compromised patients’ personal and medical info	https://www.comparitech.com/news/boston-clinic-notifies-185000-people-of-data-breach-that-compromised-patients-personal-and-medical-info/?&web_view=true
Radiology Associates of Richmond data breach impacts 1.4 million people	https://securityaffairs.com/180128/data-breach/radiology-associates-of-richmond-data-breach-impacts-1-4-million-people.html?&web_view=true
Snake Keylogger Evades Windows Defender and Scheduled Tasks to Harvest Login Credentials	https://cybersecuritynews.com/snake-keylogger-evades-windows-defender/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
SharePoint zero-day CVE-2025-53770 actively exploited in the wild	https://securityaffairs.com/180182/hacking/sharepoint-zero-day-cve-2025-53770-actively-exploited-in-the-wild.html
Microsoft SharePoint servers under attack via zero-day vulnerability with no patch (CVE-2025-53770)	https://www.helpnetsecurity.com/2025/07/20/microsoft-sharepoint-servers-under-attack-via-zero-day-vulnerability-with-no-patch-cve-2025-53770/
Fortinet FortiWeb flaw CVE-2025-25257 exploited hours after PoC release	https://securityaffairs.com/180118/hacking/fortinet-fortiweb-flaw-cve-2025-25257-exploited-hours-after-poc-release.html
Hackers Exploit Critical CrushFTP Flaw to Gain Admin Access on Unpatched Servers	https://thehackernews.com/2025/07/hackers-exploit-critical-crushftp-flaw.html
Microsoft SharePoint servers under attack via zero-day vulnerability (CVE-2025-53770)	https://www.helpnetsecurity.com/2025/07/20/microsoft-sharepoint-servers-under-attack-via-zero-day-vulnerability-with-no-patch-cve-2025-53770/
Microsoft: Windows Server KB5062557 causes cluster, VM issues	https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-server-kb5062557-causes-cluster-vm-issues/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Patches 'ToolShell' Zero-Days Exploited to Hack SharePoint Servers	https://www.securityweek.com/microsoft-patches-toolshell-zero-days-exploited-to-hack-sharepoint-servers/
Microsoft Releases Urgent Patch for SharePoint RCE Flaw Exploited in Ongoing Cyber Attacks	https://thehackernews.com/2025/07/microsoft-releases-urgent-patch-for.html

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Iranian Hackers Deploy New Android Spyware Version	https://www.infosecurity-magazine.com/news/iran-hackers-new-android-spyware/
HPE warns of hardcoded passwords in Aruba access points	https://www.bleepingcomputer.com/news/security/hpe-warns-of-hardcoded-passwords-in-aruba-access-points/
Singapore warns China-linked group UNC3886 targets its critical infrastructure	https://securityaffairs.com/180179/uncategorized/singapore-warns-china-linked-group-unc3886-targets-its-critical-infrastructure.html
SquidLoader Malware Campaign Hits Hong Kong Financial Firms	https://hackread.com/squidloader-malware-hits-hong-kong-financial-firms/

Guides / Tools

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

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/