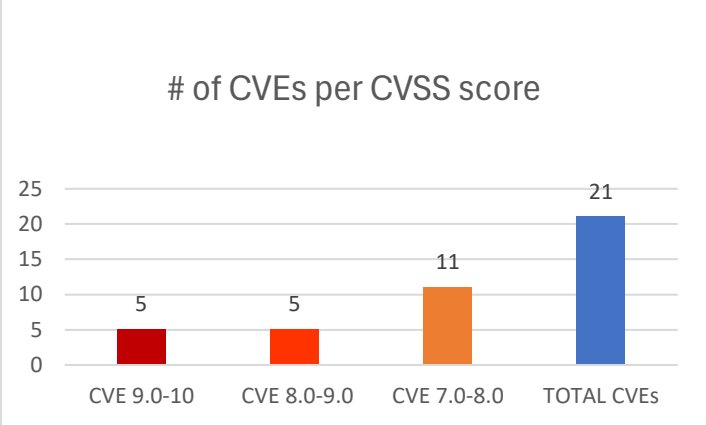
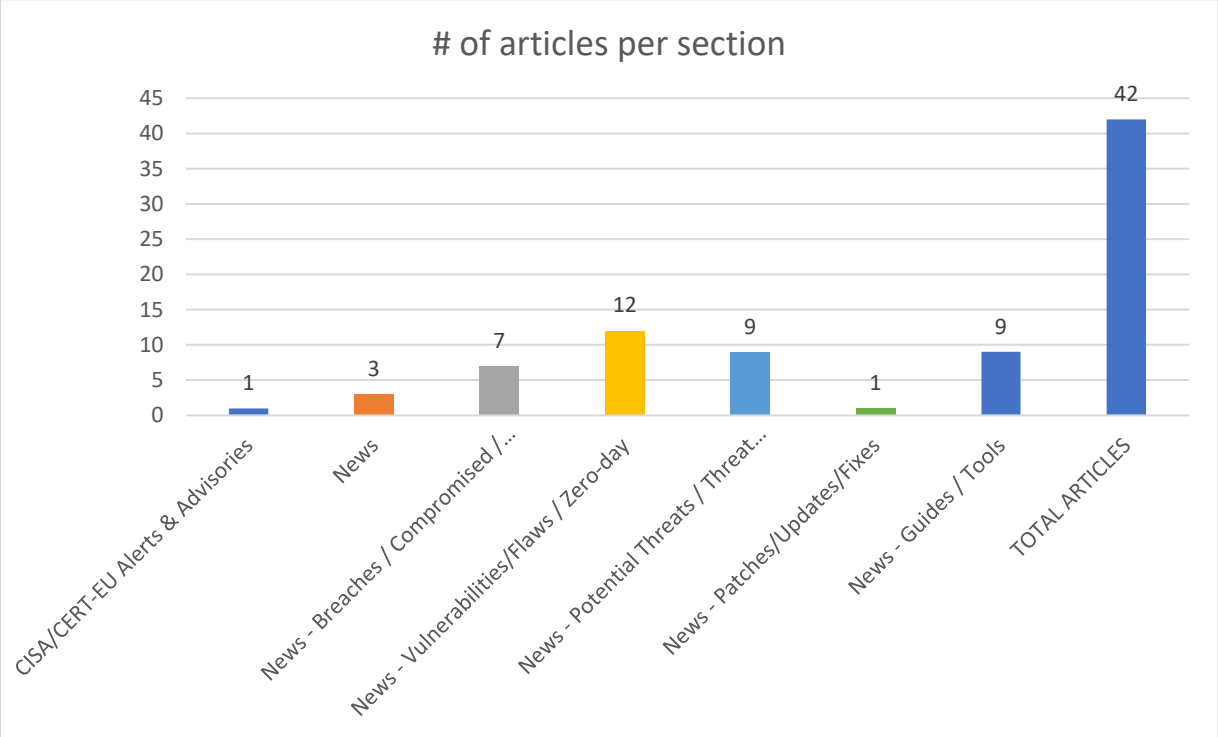
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 22/11/2025 - 25/11/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

Η ενότητα αυτή εστιάζει σε ευπάθειες που έχουν καταχωρηθεί πρόσφατα και αξιολογούνται ως σοβαρές, με βάση τη βαθμολογία CVSS. Παρουσιάζονται με σαφήνεια τα συστήματα ή εφαρμογές που επηρεάζονται, ο τύπος της ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

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-2025-64693	9,8	Security Point (Windows) of MaLion and MaLionCloud	Heap-based Buffer Overflow		https://jvn.jp/en/jp/JVN76298784/ JPCERT/CC https://www.intercom.co.jp/information/2025/1125.html
https://nvd.nist.gov/vuln/detail/CVE-2025-63958	9,8	MILLENSYS Vision Tools Workspace	Improper Access Control	6.5.0.2585	https://ozex.gitlab.io/tricks_hacks/2025-11-19-cve-2025-63958/index.html MITRE https://www.millensys.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-6389	9,8	The Sneeit Framework plugin for WordPress	Improper Control of Generation of Code ('Code Injection')	up to, and including, 8.3	https://themeforest.net/item/flat-news-responsive-magazine-wordpress-theme/6000513#item-description release-notes Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b5ed8a39-50b0-4acf-9054-ba389c49f345?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9803	9,3	lunary-ai/lunary	Improper Authentication	1.9.34	https://github.com/lunary-ai/lunary/commit/95a2cc8e012bf5f089edbfa072ba66dcb7e10d91 huntr.dev https://huntr.com/bounties/4734f35f-514c-4d10-98fa-3a54514f6af6
https://nvd.nist.gov/vuln/detail/CVE-2025-12977	9,1	Fluent Bit in_http	Improper Validation of Specified Type of Input		https://fluentbit.io/announcements/v4.1.0/
https://nvd.nist.gov/vuln/detail/CVE-2025-63434	8,8	Xtooltech Xtool AnyScan Android Application	Download of Code Without Integrity Check	4.40.40 and prior	https://github.com/ab3lson/cve-references/tree/master/CVE-2025-63434 MITRE https://www.nowsecure.com/blog/2025/07/16/remote-code-execution-discovered-in-xtool-anyscan-app-risks-to-phones-and-vehicles/

https://nvd.nist.gov/vuln/detail/CVE-2025-13551	**8,8**	D-Link	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	DIR-822K and DWR-M920 1.00_20250513 164613/1.1.50	https://github.com/QIU-DIE/CVE/issues/35 CISA-ADP, VulDB https://github.com/QIU-DIE/CVE/issues/46 CISA-ADP, VulDB https://vuldb.com/?ctiid.333318 VulDB https://vuldb.com/?id.333318 VulDB https://vuldb.com/?submit.693785 VulDB https://vuldb.com/?submit.695436 VulDB https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-65951	**8,7**	Inside Track / Entropy Derby	Use of a Broken or Risky Cryptographic Algorithm		https://github.com/mescuwa/entropy-derby/commit/2d38d2f16bbb3b4240698148f80d8c5202725c77 GitHub, Inc. https://github.com/mescuwa/entropy-derby/security/advisories/GHSA-pm54-f847-w4mh
https://nvd.nist.gov/vuln/detail/CVE-2025-10555	**8,7**	Service Items Management in DELMIA Service Process Engineer on Release 3DEXPERIENCE R2025x	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		https://www.3ds.com/trust-center/security/security-advisories/cve-2025-10555
https://nvd.nist.gov/vuln/detail/CVE-2025-62155	**8,5**	New API	Server-Side Request Forgery (SSRF)	Prior to version 0.9.6	https://github.com/QuantumNous/new-api/security/advisories/GHSA-9f46-w24h-69w4
https://nvd.nist.gov/vuln/detail/CVE-2025-7402	**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')	up to, and including, 4.95	https://codecanyon.net/item/ads-pro-plugin-multipurpose-wordpress-advertising-manager/10275010 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/5548b97d-14f0-4f50-b213-a19c02c240be?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-65998	**7,5**	Apache Syncope	Use of Hard-coded Cryptographic Key		http://www.openwall.com/lists/oss-security/2025/11/24/1 CVE https://lists.apache.org/thread/fjh0tb0d1xkbphc5ogdsc348ppz88cts
https://nvd.nist.gov/vuln/detail/CVE-2025-65503	**7,5**	Redboltz async_mqtt	Use After Free	10.2.5	https://github.com/redboltz/async_mqtt/issues/436 MITRE https://github.com/redboltz/async_mqtt/pull/437

https://nvd.nist.gov/vuln/detail/CVE-2025-65495	7,5	tls_verify_call_back() in src/coap_openssl.c in OISM libcoap	Signed to Unsigned Conversion Error	4.3.5	https://github.com/obgm/libcoap/issues/1744 MITRE https://github.com/obgm/libcoap/pull/1750
https://nvd.nist.gov/vuln/detail/CVE-2025-13384	7,5	The CP Contact Form with PayPal plugin for WordPress	Missing Authorization	up to, and including, 1.3.56	https://plugins.trac.wordpress.org/browser/cp-contact-form-with-paypal/tags/1.3.56/cp_contact-formpp_functions.php#L541 Wordfence https://plugins.trac.wordpress.org/browser/cp-contact-form-with-paypal/tags/1.3.56/cp_contact-formpp_functions.php#L877 Wordfence https://plugins.trac.wordpress.org/browser/cp-contact-form-with-paypal/tags/1.3.56/cp_contact-formpp_functions.php#L925 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3399104%40cp-contact-form-with-paypal&new=3399104%40cp-contact-form-with-paypal&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/6639c3d8-8f26-4ee5-8c4b-2efcf34668a2?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13502	7,5	WebKitGTK and WPE WebKit	Integer Overflow or Wraparound		https://access.redhat.com/security/cve/CVE-2025-13502 Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2416300
https://nvd.nist.gov/vuln/detail/CVE-2025-13556	7,3	Campcodes Online Polling System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/ProgramShowMaker/CVE/issues/2 CISA-ADP, VulDB https://vuldb.com/?ctiid.333323 VulDB https://vuldb.com/?id.333323 VulDB https://vuldb.com/?submit.696614 VulDB https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-13555	7,3	Campcodes School File Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/arpcyber070/CVE/issues/4 CISA-ADP, VulDB https://vuldb.com/?ctiid.333322 VulDB https://vuldb.com/?id.333322 VulDB

					https://vuldb.com/?submit.696516 VulDB https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-13376	**7,2**	The ProjectList plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 0.3.0	https://plugins.trac.wordpress.org/browser/project-list/tags/0.3.0/pages/pl-add.php#L27 Wordfence https://plugins.trac.wordpress.org/browser/project-list/trunk/pages/pl-add.php#L27 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/781c3b84-df80-470e-8bcb-3305a8bbb64a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-65018	**7,1**	LIBPNG	Heap-based Buffer Overflow	From version 1.6.0 to before 1.6.51	https://github.com/pnggroup/libpng/commit/16b5e3823918840aae65c0a6da57c78a5a496a4d GitHub, Inc. https://github.com/pnggroup/libpng/commit/218612ddd6b17944e21eda56caf8b4bf7779d1ea GitHub, Inc. https://github.com/pnggroup/libpng/issues/755 GitHub, Inc. https://github.com/pnggroup/libpng/pull/757 GitHub, Inc. https://github.com/pnggroup/libpng/security/advisories/GHSA-7wv6-48j4-hj3g
https://nvd.nist.gov/vuln/detail/CVE-2025-12629	**7,1**	The Broken Link Manager WordPress plugin		0.6.5	https://wpscan.com/vulnerability/528e9775-3a2d-4e52-92f7-f123ad787e7d/

CISA/CERT-EU Alerts & Advisories

Αυτό το κομμάτι περιλαμβάνει ειδοποιήσεις από επίσημες πηγές, κυρίως CISA και CERT-EU, σχετικά με κρίσιμες ευπάθειες ή ενεργές απειλές. Συνήθως αφορούν βιομηχανικά ή κρίσιμα συστήματα, αλλά και mainstream λογισμικό. Προσφέρονται σε μορφή σύντομων αναφορών και οδηγούν σε πιο λεπτομερείς τεχνικές οδηγίες.

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Spyware Allows Cyber Threat Actors to Target Users of Messaging Applications		**https://www.cisa.gov/news-events/alerts/2025/11/24/spyware-allows-cyber-threat-actors-target-users-messaging-applications**

News

Η ενότητα "News" συνοψίζει τα πιο σημαντικά γεγονότα της εβδομάδας στον τομέα της κυβερνοασφάλειας. Εδώ θα βρείτε επιθέσεις που ξεχώρισαν, νέες τεχνικές που εντοπίστηκαν, ή ενέργειες από γνωστές ομάδες hacking. Δίνει την απαραίτητη εικόνα του τι συμβαίνει διεθνώς και πού πρέπει να στραφεί η προσοχή.

Σύντομη περιγραφή / Τίτλος	URL
Russian-linked Malware Campaign Hides in Blender 3D Files	https://www.infosecurity-magazine.com/news/russian-malware-blender-3d-files/
Beware of North Korean Fake Job Platform Targeting U.S. Based AI-Developers	https://cybersecuritynews.com/beware-of-north-korean-fake-job-platform/
APT35 Hacker Groups Internal Documents Leak Exposes their Targets and Attack Methods	https://cybersecuritynews.com/apt35-hacker-groups-internal-documents/

Breaches / Compromised / Hacked

Καταγράφονται περιπτώσεις παραβίασης δεδομένων, διαρροών και άλλων σοβαρών περιστατικών ασφαλείας. Περιλαμβάνονται πληροφορίες για το ποιοι επηρεάστηκαν, με ποιον τρόπο έγινε η παραβίαση και πού υπάρχουν διαθέσιμες λεπτομέρειες. Είναι μια χρήσιμη εικόνα για να αντιληφθεί κανείς τη δυναμική των επιθέσεων σε πραγματικές συνθήκες.

Σύντομη περιγραφή / Τίτλος	URL
ShinyHunters Claims Data Theft from 200+ Companies via Salesforce Gainsight Breach	https://cybersecuritynews.com/shinyhunters-salesforce-gainsight-breach/
Massive data leak hits Italian railway operator Ferrovie dello Stato via Almaviva hack	https://securityaffairs.com/184907/data-breach/massive-data-leak-hits-italian-railway-operator-ferrovie-dello-stato-via-almaviva-hack.html?&web_view=true

Cox Enterprises discloses Oracle E-Business Suite data breach	https://www.bleepingcomputer.com/news/security/cox-enterprises-discloses-oracle-e-business-suite-data-breach/?&web_view=true
Iberia Airlines Notifies Customers of Supply Chain Data Breach	https://www.infosecurity-magazine.com/news/iberia-airlines-supply-chain-data/
Zapier's NPM Account Hacked – Multiple Packages Infected with Self-Propagating Shai Hulud Malware	https://cybersecuritynews.com/zapiers-npm-account-compromised/
PoC released for W3 Total Cache Vulnerability that Exposes 1+ Million Websites to RCE Attacks	https://cybersecuritynews.com/poc-released-for-w3-total-cache-vulnerability/
Sha1-Hulud Supply Chain Attack: 800+ npm Packages and Thousands of GitHub Repos Compromised	https://cybersecuritynews.com/sha1-hulud-supply-chain-attack/

Vulnerabilities / Flaws / Zero-day

Αναφέρονται τεχνικά ελαττώματα ή αδυναμίες που ενδέχεται να αξιοποιηθούν άμεσα από επιτιθέμενους — είτε επειδή είναι zero-day είτε γιατί η διόρθωσή τους καθυστερεί. Περιλαμβάνονται περιπτώσεις όπου δεν απαιτείται αλληλεπίδραση με τον χρήστη ή όπου παρακάμπτονται βασικά μέτρα ασφαλείας. Πολύ χρήσιμο για ομάδες που ασχολούνται με threat detection.

Σύντομη περιγραφή / Τίτλος	URL
ShadowPad Malware Actively Exploits WSUS Vulnerability for Full System Access	https://thehackernews.com/2025/11/shadowpad-malware-actively-exploits.html
CISA Warns of Actively Exploited Critical Oracle Identity Manager Zero-Day Vulnerability	https://thehackernews.com/2025/11/cisa-warns-of-actively-exploited.html
DeepSeek-R1 Makes Code for Prompts With Severe Security Vulnerabilities	https://cybersecuritynews.com/deepseek-r1-code-vulnerabilities/
Wireshark Vulnerabilities Let Attackers Crash by Injecting a Malformed Packet	https://cybersecuritynews.com/wireshark-vulnerabilities-4-6-1/
Critical Vulnerability in Azure Bastion Let Attackers Bypass Authentication and Escalate privileges	https://cybersecuritynews.com/azure-bastion-vulnerability/
Microsoft Confirms Windows 11 24H2 Update Broken Multiple Core Features	https://cybersecuritynews.com/windows-11-24h2-features-broken/
Metasploit Adds Exploit Module for Recently Disclosed FortiWeb 0-Day Vulnerabilities	https://cybersecuritynews.com/metasploit-module-fortiweb-0-day/
Critical Oracle Identity Manager Flaw Possibly Exploited as Zero-Day	https://www.securityweek.com/critical-oracle-identity-manager-flaw-possibly-exploited-as-zero-day/
NVIDIA's Isaac-GROOT Robotics Platform Vulnerability Let Attackers Inject Malicious Codes	https://cybersecuritynews.com/nvidias-isaac-groot-robotics-platform-vulnerability/
Flaws Expose Risks in Fluent Bit Logging Agent	https://www.infosecurity-magazine.com/news/flaws-expose-risks-fluent-bit/
vLLM Vulnerability Enables Remote Code Execution Via Malicious Payloads	https://cybersecuritynews.com/vllm-vulnerability-enables-remote-code-execution/
Tenda N300 Vulnerabilities Let Attacker to Execute Arbitrary Commands as Root User	https://cybersecuritynews.com/tenda-n300-vulnerabilities/

Patches / Updates / Fixes

Εδώ θα βρείτε τις πιο πρόσφατες διορθώσεις και ενημερώσεις ασφαλείας από προμηθευτές λογισμικού και hardware. Το περιεχόμενο αφορά συγκεκριμένα bugs ή exploits που έχουν ήδη δημοσιοποιηθεί, μαζί με οδηγίες για το πώς να εφαρμοστούν τα patches.

Σύντομη περιγραφή / Τίτλος	URL
CISA Urges Patch of Actively Exploited Flaw in Oracle Identity Manager	https://www.infosecurity-magazine.com/news/cisa-kev-oracle-identity-manager/

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συν-θήκες. Περιλαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
ShadowRay 2.0 Turns AI Clusters into Crypto Botnets	https://www.darkreading.com/cyber-risk/shadowray-20-ai-clusters-crypto-botnets
ClickFix Attack Uses Steganography to Hide Malicious Code in Fake Windows Security Update Screen	**https://cybersecuritynews.com/fake-windows-security-update-screen/**
Hackers Replace 'm' with 'rn' in Microsoft(.)com to Steal Users' Login Credentials	https://cybersecuritynews.com/microsoft-phishing-replace-m-with-rn/
Threats Actors Leverage Python-based Malware to Inject Process into a Legitimate Windows Binary	https://cybersecuritynews.com/threats-actors-leverage-python-based-malware/
Hackers Leveraging WhatsApp to Silently Install Malware to Harvest Logs and Contact Details	https://cybersecuritynews.com/hackers-leveraging-whatsapp/
Dropping Elephant Hacker Group Attacks Defense Sector Using Python Backdoor via MSBuild Dropper	https://cybersecuritynews.com/dropping-elephant-hacker-group-attacks-defense-sector/
LLMs Tools Like GPT-3.5-Turbo and GPT-4 Fuels the Development of Fully Autonomous Malware	https://cybersecuritynews.com/llms-tools-like-gpt-3-5-turbo-and-gpt-4/
Hackers Leverage Malicious PyPI Package to Attack Users and Steal Cryptocurrency Details	https://cybersecuritynews.com/hackers-leverage-malicious-pypi-package/
New EtherHiding Attack Uses Web-Based Attacks to Deliver Malware and Rotate Payloads	https://cybersecuritynews.com/new-etherhiding-attack-uses-web-based-attacks/

Guides / Tools

Παρουσιάζονται τεχνικοί οδηγοί και εργαλεία που μπορούν να βοηθήσουν στην παρακολούθηση, ανάλυση ή ενίσχυση της ασφάλειας συστημάτων. Είτε πρόκειται για open source projects είτε για νέες τεχνικές, η ενότητα αυτή λειτουργεί ως πόρος για πρακτικές λύσεις στην καθημερινή δουλειά των επαγγελματιών ασφάλειας.

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/
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
Top 15 Best Security Incident Response Tools In 2025	https://cybersecuritynews.com/incident-response-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-tools/
ThreatBook Launches Best-of-Breed Advanced Threat Intelligence Solution	https://cybersecuritynews.com/threatbook-advanced-threat-intelligence-solution/
CISA Releases Best Security Practices Guide for Hardening Microsoft Exchange Server	https://cybersecuritynews.com/microsoft-exchange-server-hardening-guide/
15 Best Remote Monitoring Tools – 2025	https://cybersecuritynews.com/best-remote-monitoring-tools/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-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/