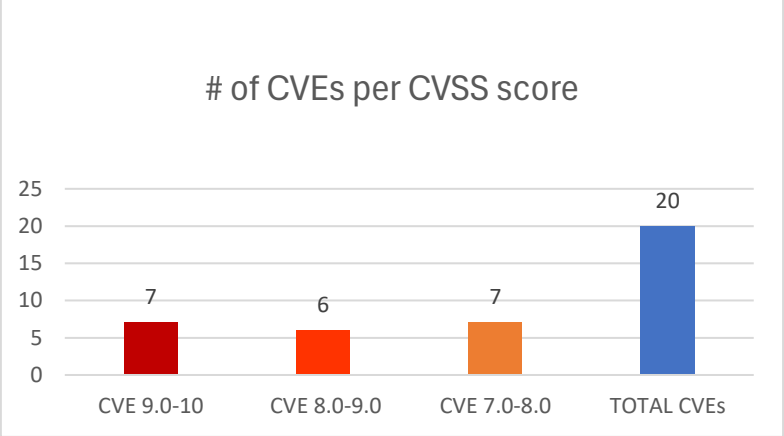
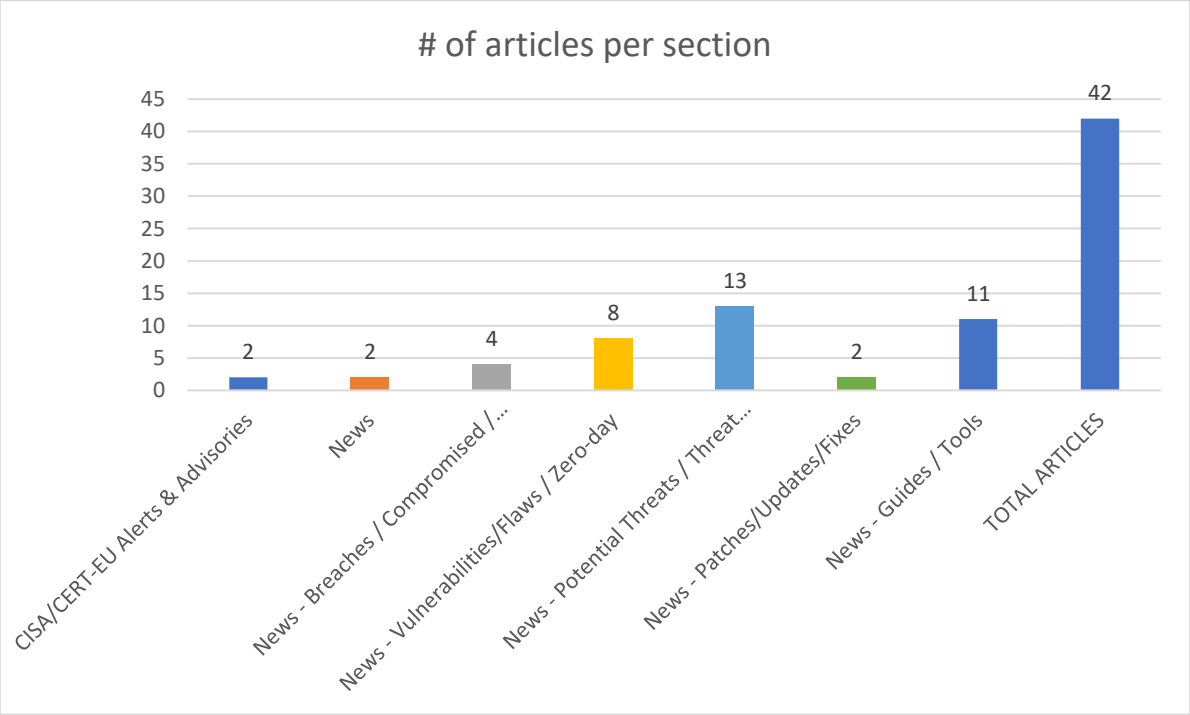
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 20/05/2026 - 22/05/2026





Contents

Common Vulnerabilities and Exposures (CVEs)

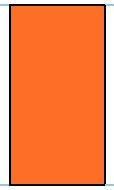
Η ενότητα αυτή εστιάζει σε ευπάθειες που έχουν καταχωρηθεί πρόσφατα και αξιολογούνται ως σοβαρές, με βάση τη βαθμολογία CVSS. Παρουσιάζονται με σαφήνεια τα συστήματα ή εφαρμογές που επηρεάζονται, ο τύπος της ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση 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-2026-4858	9,9	Mattermost	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11.6.x <= 11.6.0, 11.5.x <= 11.5.3, 11.4.x <= 11.4.4, 10.11.x <= 10.11.14	https://mattermost.com/security-updates
https://nvd.nist.gov/vuln/detail/CVE-2026-24207	9,8	NVIDIA Triton Inference Server	Authentication Bypass Using an Alternate Path or Channel		https://nvd.nist.gov/vuln/detail/CVE-2026-24207 NVIDIA Corporation Third Party Advisory US Government Resource https://nvidia.custhelp.com/app/answers/detail/a_id/5828 NVIDIA Corporation Vendor Advisory https://www.cve.org/CVERecord?id=CVE-2026-24207
https://nvd.nist.gov/vuln/detail/CVE-2026-33278	9,8	NLnet Labs Unbound	Operation on a Resource after Expiration or Release	1.19.1 up to and including version 1.25.0	https://www.nlnetlabs.nl/downloads/unbound/CVE-2026-33278.txt
https://nvd.nist.gov/vuln/detail/CVE-2026-8631	9,8	HP Linux Imaging and Printing Software	Heap-based Buffer Overflow		https://support.hp.com/us-en/document/ish_14942099-14942126-16/hpsbpi04118
https://nvd.nist.gov/vuln/detail/CVE-2026-6960	9,8	The BookingPress Pro plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 5.6	https://www.bookingpressplugin.com/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/ed738dc5-7848-4b04-a3fd-317cc366acfa?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2026-3593	9,8	the DNS-over-HTTPS	Use After Free	BIND 9 versions 9.20.0 through 9.20.22, 9.21.0 through 9.21.21, and 9.20.9-S1 through 9.20.22-S1	https://downloads.isc.org/isc/bind9/9.20.23 Internet Systems Consortium (ISC) Patch https://downloads.isc.org/isc/bind9/9.21.22 Internet Systems Consortium (ISC) Patch https://kb.isc.org/docs/cve-2026-3593
https://nvd.nist.gov/vuln/detail/CVE-2025-31973	9,8	HCL BigFix Service Management (SM)	Insufficient Information		https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0128144
https://nvd.nist.gov/vuln/detail/CVE-2026-9120	8,8	WebRTC in Google Chrome	Use After Free	prior to 148.0.7778.179	https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html Chrome Vendor Advisory https://issues.chromium.org/issues/504620824
https://nvd.nist.gov/vuln/detail/CVE-2026-47102	8,8	LiteLLM	Incorrect Authorization	prior to 1.83.10	https://gist.github.com/13ph03nix/9ec616e1fdc77b3673509c60206e827f VulnCheck https://github.com/BerriAI/litellm/commit/128d32d2494b759c5d15da3452452af4c6a34c01 VulnCheck https://github.com/BerriAI/litellm/commit/e6f18ce75b111c9b93dc15c72894cbdeb53177ce VulnCheck https://github.com/BerriAI/litellm/pull/25541 VulnCheck https://github.com/BerriAI/litellm/releases/tag/v1.83.10-stable VulnCheck https://huntr.com/bounties/8e75edfb-ff05-4e63-bfca-2d93d03fb3b9 VulnCheck https://www.vulncheck.com/advisories/litellm-privilege-escalation-via-user-update

https://nvd.nist.gov/vuln/detail/CVE-2026-44925	8,8	InfoScale Operations Manager (VIOM)	Cross-Site Request Forgery (CSRF)	v.9.1.3	https://supportinfoscale.cloud.com/support-home/kbsearch/article?articleNumber=1000766080&articleTitle=InfoScale_Operations_Manager_IOM_web_application_Security_Bulletin_for_CVE_2026_44923_CVE_2026_44924_and_CVE_2026_44925 MITRE Vendor Advisory https://www.veritas.com/support/en_US/doc/120571566-166757640-0/viom_tot_v118836641-166757640
https://nvd.nist.gov/vuln/detail/CVE-2026-24217	8,8	NVIDIA BioNeMo Core for Linux	Path Traversal: '\..\filename'		https://nvd.nist.gov/vuln/detail/CVE-2026-24217 NVIDIA Corporation US Government Resource https://nvidia.custhelp.com/app/answers/detail/a_id/5831 NVIDIA Corporation Vendor Advisory https://www.cve.org/CVERecord?id=CVE-2026-24217
https://nvd.nist.gov/vuln/detail/CVE-2026-45584	8,1	Microsoft Defender	Heap-based Buffer Overflow		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45584
https://nvd.nist.gov/vuln/detail/CVE-2026-47784	8,1	memcached	Observable Timing Discrepancy	before 1.6.42	https://github.com/memcached/memcached/commit/d13f282b4bce33a9c33b8a1bbf07f12114160fed MITRE Patch https://github.com/memcached/memcached/compare/1.6.41...1.6.42 MITRE Release Notes https://github.com/memcached/memcached/wiki/ReleaseNotes1642
https://nvd.nist.gov/vuln/detail/CVE-2026-45250	7,8	The setcred(2)	Stack-based Buffer Overflow		http://www.openwall.com/lists/oss-security/2026/05/21/18 CVE http://www.openwall.com/lists/oss-security/2026/05/21/3 CVE http://www.openwall.com/lists/oss-security/2026/05/22/5 CVE https://security.freebsd.org/advisories/FreeBSD-SA-26:18.setcred.asc

https://nvd.nist.gov/vuln/detail/CVE-2026-8486	7,5	Progress Software MOVEit Automation	Allocation of Resources Without Limits or Throttling	before 2025.0.11, from 2025.1.0 before 2025.1.7.	https://docs.progress.com/bundle/moveit-automation-release-notes-2026/page/Fixed-Issues-2026.html
https://nvd.nist.gov/vuln/detail/CVE-2026-9117	7,5	GFX in Google Chrome on Linux, ChromeOS	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 148.0.7778.179	https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html Chrome Vendor Advisory https://issues.chromium.org/issues/497542537
https://nvd.nist.gov/vuln/detail/CVE-2026-4834	7,5	The WP ERP Pro plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 1.5.1.	https://wperp.com/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/d3849db8-5c9e-410e-be53-c9ab76162630?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-46473	7,5	Authen::TOTP	Insufficient Entropy	before 0.1.1	http://www.openwall.com/lists/oss-security/2026/05/21/15 CVE https://github.com/tchatzi/Authen-TOTP/commit/d04f30cc6538d77fc6b6d550da450cf3017b8561.patch CPANSec https://metacpan.org/release/TCHATZI/Authen-TOTP-0.1.1/changes
https://nvd.nist.gov/vuln/detail/CVE-2026-20239	7,5	Splunk	Insertion of Sensitive Information into Log File	Enterprise versions below 10.2.2 and 10.0.5, and Splunk Cloud Platform versions below 10.3.2512.8, 10.2.2510.11, 10.1.2507.21, and 10.0.2503.13	https://advisory.splunk.com/advisories/SVD-2026-0503
https://nvd.nist.gov/vuln/d	7,0	Rsync	Time-of-check Time-of-use	before 3.4.3	https://github.com/RsyncProject/rsync/pull/895/changes/8471fdd1561049ef5f58df44a1811a50bd9a531d VulnCheck Patch

etail/CVE-2026-29518		(TOCTOU) Race Condition		https://github.com/RsyncProject/rsync/releases/tag/v3.4.3 VulnCheck Release Notes https://www.vulncheck.com/advisories/rsync-toctou-race-condition-allows-symlink-based-arbitrary-file-write

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
CISA Adds Seven Known Exploited Vulnerabilities to Catalog	▪ **CVE-2008-4250 Microsoft Windows Buffer Overflow Vulnerability** ▪ **CVE-2009-1537 Microsoft DirectX NULL Byte Overwrite Vulnerability** ▪ **CVE-2009-3459 Adobe Acrobat and Reader Heap-Based Buffer Overflow Vulnerability** ▪ **CVE-2010-0249 Microsoft Internet Explorer Use-After-Free Vulnerability** ▪ **CVE-2010-0806 Microsoft Internet Explorer Use-After-Free Vulnerability** ▪ **CVE-2026-41091 Microsoft Defender Elevation of Privilege Vulnerability** ▪ **CVE-2026-45498 Microsoft Defender Denial of Service Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/05/20/cisa-adds-seven-known-exploited-vulnerabilities-catalog**
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-34291 Langflow Origin Validation Error Vulnerability ▪ CVE-2026-34926 Trend Micro Apex One (On-Premise) Directory Traversal Vulnerability	**https://www.cisa.gov/news-events/alerts/2026/05/21/cisa-adds-two-known-exploited-vulnerabilities-catalog**

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
Cybercriminal VPN Dismantled in Europol Crackdown	https://www.infosecurity-magazine.com/news/first-vpn-takedown-europol/
Three-Quarters of Firms Knowingly Ship Vulnerable Code	https://www.infosecurity-magazine.com/news/threequarters-knowingly-ship/

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
GitHub Confirms Breach, 4K Internal Repos Stolen	https://www.darkreading.com/application-security/github-confirms-breach-4k-internal-repos-stolen
Grafana GitHub Breach Linked to TanStack npm Supply Chain Ransomware	https://cybersecuritynews.com/grafana-github-breach-linked-tanstack-ransomware/
Megalodon Malware Compromised 5,500+ GitHub Repos Within 6 Hours	https://cybersecuritynews.com/megalodon-malware-github-repos/
P2PInfect Botnet Compromises Kubernetes Clusters Through Exposed Redis Instances	https://cybersecuritynews.com/p2pinfect-botnet-compromises-kubernetes-clusters-through-exposed-redis-instances/

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
9-Year-Old Linux Kernel Flaw Enables Root Command Execution on Major Distros	https://thehackernews.com/2026/05/9-year-old-linux-kernel-flaw-enables.html
Highly Critical Drupal Core Flaw Exposes PostgreSQL Sites to RCE Attacks	https://thehackernews.com/2026/05/highly-critical-drupal-core-flaw.html
Patch Now: Critical Flaw in OT Robot OS Gives Attackers Control	https://www.darkreading.com/ics-ot-security/patch-now-critical-flaw-ot-robot-os
Hackers bypass SonicWall VPN MFA due to incomplete patching	https://www.bleepingcomputer.com/news/security/hackers-bypass-sonicwall-vpn-mfa-due-to-incomplete-patching/
Verizon DBIR: Vulnerability Exploits Overtake Credentials as Top Access Vector	https://www.infosecurity-magazine.com/news/verizon-dbir-exploits-top-access/
Claude Code's Network Sandbox Vulnerability Exposes User Credentials and Source Code	https://cybersecuritynews.com/claude-codes-network-sandbox-vulnerability/
New NGINX Vulnerability Allows Remote Attackers to Trigger Malicious Code	https://cybersecuritynews.com/nginx-buffer-overflow-vulnerability/
Critical Cisco Secure Workload Vulnerability Enables Unauthorized API Access	https://cybersecuritynews.com/cisco-secure-workload-vulnerability/

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
Microsoft Releases Mitigation for YellowKey BitLocker Bypass CVE-2026-45585 Exploit	https://thehackernews.com/2026/05/microsoft-releases-mitigation-for.html
Google Publishes Exploit Code for Unfixed Chromium Bug Exposing Millions of Users	https://cybersecuritynews.com/google-publishes-chromium-exploit-code/

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
Researchers Warn CypherLoc Scareware Has Targeted Millions of Users	https://www.infosecurity-magazine.com/news/researchers-cypherloc-scareware/
China-Linked Webworm APT Evolves Tactics, Expands to European Targets	https://www.infosecurity-magazine.com/news/webworm-apt-evolves-tactics/
Android Malware Campaign Used Hundreds of Fake Apps to Silently Charge Users	https://www.infosecurity-magazine.com/news/android-carrier-billing-fraud-four/
Mini Shai-Hulud Hits Hundreds of npm Packages in AntV Ecosystem	https://www.infosecurity-magazine.com/news/antv-npm-mini-shai-hulud-largest/
WantToCry Ransomware Abuses SMB Services to Remotely Encrypt Files	https://cybersecuritynews.com/wanttocry-ransomware-abuses-smb-services/
Gremlin Stealer Stores C2 URLs and Exfiltration Paths in Encrypted Resource Sections	https://cybersecuritynews.com/gremlin-stealer-stores-c2-urls/
PinTheft Linux Vulnerability Let Attackers Gain Root Access – PoC Released	https://cybersecuritynews.com/pintheft-linux-vulnerability/
Fox Tempest Malware-Signing Service Abused Microsoft Artifact Signing to Certify Malware	https://cybersecuritynews.com/fox-tempest-abuse-microsoft-artifact-signing/
Mini Shai-Hulud Attack Forces npm to Reset Bypass-2FA Publishing Tokens	https://cybersecuritynews.com/mini-shai-hulud-attack-forces-npm/
Fake Invitation Phishing Campaign Targets U.S. Organizations With Credential Theft	https://cybersecuritynews.com/fake-invitation-phishing-campaign/
Indian Student Data Weaponized for Phishing, Social Engineering, and Financial Fraud	https://cybersecuritynews.com/indian-student-data-weaponized-for-phishing/
Hackers Use Fake Microsoft Teams Downloads to Deploy ValleyRAT Malware	https://cybersecuritynews.com/hackers-use-fake-microsoft-teams-downloads-to-deploy-valleyrat-malware/
Hackers Can Weaponize Lenovo Driver to Terminate EDR Processes	https://cybersecuritynews.com/lenovo-driver-terminate-edr-processes/

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/**
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
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/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-management-tools/
NETREAPER Offensive Security Toolkit That Wraps 70+ Penetration Testing Tools	https://cybersecuritynews.com/netreaper-offensive-security-toolkit/
GitLab Security Best Practices Cheat Sheet	https://thehackernews.uk/gitlab-security-tips
False Negatives Are a New SOC Headache. Here's the Fast Way to Fix It	https://cybersecuritynews.com/false-negatives-are-a-new-soc-headache-heres-the-fast-way-to-fix-it/
PentAGI – Automated AI-Powered Penetration Testing Tool that Integrates 20+ Security Tools	https://cybersecuritynews.com/pentagi-penetration-testing-tool/
The CISO Executive Toolkit (Free Download)	https://thehackernews.uk/wiz-ciso-bundle
Secure Coding Best Practices: Practical Guide + Cheat Sheet for Developers	https://thehackernews.uk/secure-coding-wiz-cheat

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/