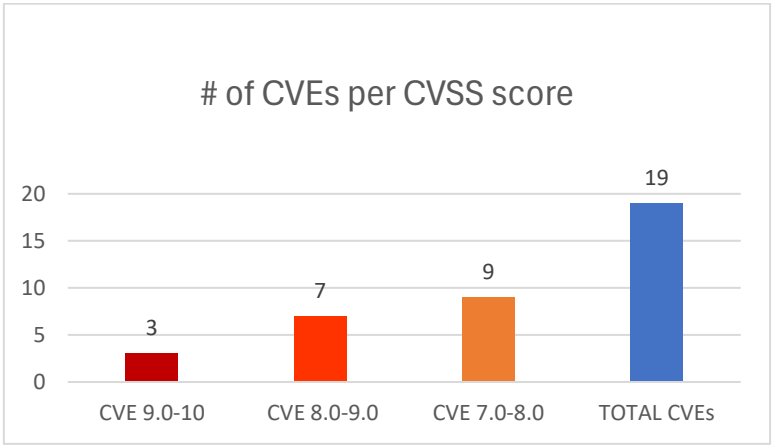
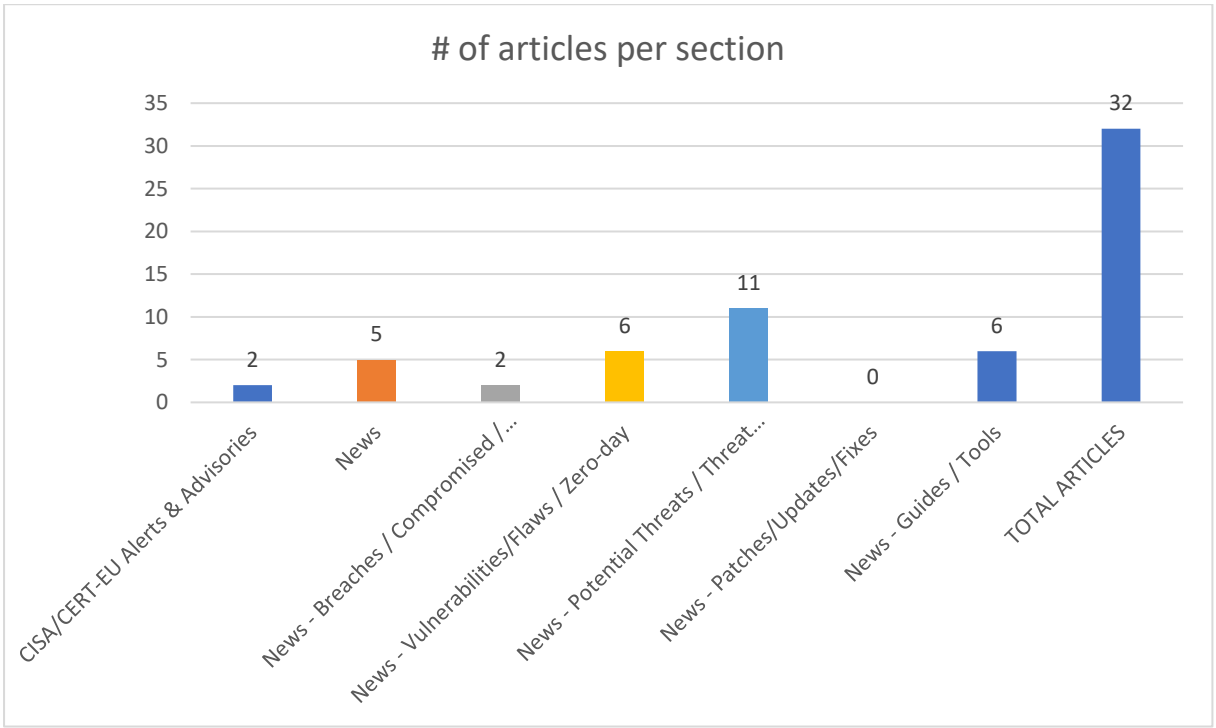
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 24/10/2025 - 27/10/2025





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-2025-60553	9,8	D-Link DIR600L Ax FW116WWb01	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		https://github.com/luckysmallbird/DLINK-DIR600LAx-Vulnerability/blob/main/03-buffer%20overflow-formSetWAN_Wizard52.md
https://nvd.nist.gov/vuln/detail/CVE-2025-43995	9,8	Dell Storage Center - Dell Storage Manager	Improper Authentication	20.1.21	https://www.dell.com/support/kbdoc/en-us/000382899/dsa-2025-393-security-update-for-storage-center-dell-storage-manager-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-11253	9,8	Aksis Technology Inc. Netty ERP	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before V.1.1000	https://www.usom.gov.tr/bildirim/tr-25-0359
https://nvd.nist.gov/vuln/detail/CVE-2025-12095	8,8	The Simple Registration for WooCommerce plugin for WordPress	Cross-Site Request Forgery (CSRF)	up to, and including, 1.5.8	https://plugins.trac.wordpress.org/browser/woocommerce-simple-registration/tags/1.5.8/includes/display-role-admin.php#L132 Wordfence https://plugins.trac.wordpress.org/changeset/3383124 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/9c32fcaf-afc3-4493-8cd8-6f49bbe40c7b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11893	8,8	The Charitable – Donation Plugin for WordPress – Fund-	Improper Neutralization of Special Elements used in	up to, and including, 1.8.8.4	https://plugins.trac.wordpress.org/browser/charitable/trunk/includes/abstracts/abstract-class-charitable-query.php#L194 Wordfence https://plugins.trac.wordpress.org/changeset/3382719/charitable/trunk/includes/abstracts/abstract-class-charitable-

		raising with Recurring Donations & More plugin for WordPress	an SQL Command ('SQL Injection')		query.php?contextall=1 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/46b7820c-f36d-4c7d-b326-07259786fc6a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-12028	8,8	The IndieAuth plugin for WordPress	Cross-Site Request Forgery (CSRF)	up to, and including, 4.5.4	https://plugins.trac.wordpress.org/browser/indieauth/tags/4.5.4/includes/class-indieauth-authorization-endpoint.php#L411 Wordfence https://plugins.trac.wordpress.org/browser/indieauth/tags/4.5.4/includes/class-indieauth-authorization-endpoint.php#L418 Wordfence https://plugins.trac.wordpress.org/browser/indieauth/tags/4.5.4/includes/class-indieauth-authorization-endpoint.php#L476 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/42b373da-d5a6-4e3b-90f4-059da3641841?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-60954	8,3	Weak Password Requirements	Microweber CMS	2.0	https://gist.github.com/progprnv/feae2b76f2db0cb2ac6e14b1bf7d8646 MITRE https://github.com/microweber/microweber MITRE https://github.com/progprnv/CVE-Reports/blob/main/CVE-2025-60954
https://nvd.nist.gov/vuln/detail/CVE-2025-46183	8,2	The Utils.deserialize function in pgCode-Keeper	Deserialization of Untrusted Data	10.12.0	https://github.com/hacktimepro/vulnerabilities/blob/main/Disclosure_CVE-2025-46183_pgcodekeeper.md
https://nvd.nist.gov/vuln/detail/CVE-2025-10488	8,1	The Directorist: AI-Powered Business Directory Plugin with Classified Ads Listings plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 8.4.8	https://plugins.trac.wordpress.org/browser/directorist/tags/8.4.5/includes/classes/class-add-listing.php#L634 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3377181%40directorist&new=3377181%40directorist&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/2249ef72-9955-4636-b32f-e88720923268?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-62868	8,1	Edge-Themes Edge CPT	Improper Control of Filename for Include/Require	from n/a through 1.4	https://vdp.patchstack.com/database/wordpress/plugin/edge-cpt/security-policy/vdp/vulnerability/wordpress-edge-cpt-plugin-1-4-local-file-inclusion-vulnerability?_s_id=cve

			Statement in PHP Program ('PHP Remote File Inclusion		
https://nvd.nist.gov/vuln/detail/CVE-2025-60730	7,6	PerfreeBlog	Incomplete Cleanup	v4.0.11	http://perfreeblog.com MITRE https://github.com/dengxmenglihua/cve/blob/main/Perfree-Blog/File%20Deletion/Arbitrary%20File%20Deletion%20Vulnerability%20in%20PerfreeBlog%20System.md MITRE https://perfree.org.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-52099	7,5	SQLite SQLite3	Integer Overflow or Wraparound	v.3.50.0	http://sqlite3.com MITRE https://github.com/SCREAMBBY/CVE-2025-52099
https://nvd.nist.gov/vuln/detail/CVE-2025-4203	7,5	The wpForo Forum plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 2.4.8	https://plugins.trac.wordpress.org/browser/wpforo/tags/2.4.5/classes/Members.php#L1557 Wordfence https://plugins.trac.wordpress.org/browser/wpforo/tags/2.4.9/classes/Members.php#L1557 Wordfence https://wordpress.org/plugins/wpforo/#developers Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/bc406e8a-c4eb-45c3-a53c-37644e0dabfa?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-8416	7,5	The Product Filter by WBW plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 2.9.7	https://plugins.trac.wordpress.org/browser/woo-product-filter/tags/2.8.6/modules/woofilters/controller.php#L136 Wordfence https://plugins.trac.wordpress.org/browser/woo-product-filter/tags/2.8.6/modules/woofilters/mod.php#L2056 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3370655%40woo-product-filter&new=3370655%40woo-product-filter&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/d1533e9a-dcb9-4fbb-a1a7-7f4dafd3a1c8?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-9322	7,5	The Stripe Payment Forms by WP Full Pay – Accept Credit Card Payments, Donations & Subscriptions plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 8.3.1	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3378785%40wp-full-stripe-free&new=3378785%40wp-full-stripe-free&sfp_email=&sfph_mail=#file6 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/886b612a-d0d1-4880-b423-eb62410a28cd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-10861	7,5	The Popup builder with Gamification, Multi-Step Popups, Page-Level Targeting, and WooCommerce Triggers plugin for WordPress	Server-Side Request Forgery (SSRF)	up to, and including, 2.1.4.	https://plugins.trac.wordpress.org/browser/popup-builder-block/tags/2.1.2/includes/Routes/FetchDemo.php#L15 Wordfence https://plugins.trac.wordpress.org/browser/popup-builder-block/tags/2.1.2/includes/Routes/FetchDemo.php#L35 Wordfence https://plugins.trac.wordpress.org/changeset/3369146/ Wordfence https://plugins.trac.wordpress.org/changeset/3379308/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/5f4767b5-5dd6-4a2a-b44a-5297432286b1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11504	7,5	The Quickcreator – AI Blog Writer plugin for WordPress	Insertion of Sensitive Information into Log File	0.0.9 to 0.1.17	https://wordpress.org/plugins/quickcreator/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/561f171e-f13e-408b-a63e-bf6a512d4463?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-8709	7,3	LangGraph's SQLite	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	version is langgraph-checkpoint-sqlite 2.0.10	https://huntr.com/bounties/9793f4b3-76f8-44a4-989f-49a2177ee118
https://nvd.nist.gov/vuln/detail/CVE-2025-11238	7,2	The Watu Quiz plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	less than, or equal to, 3.4.4	https://plugins.trac.wordpress.org/changeset/3373855/watu Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/168e7eac-21ad-43ca-93d1-73c38e12bc29?source=cve

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
Microsoft Releases Out-of-Band Security Update to Mitigate Windows Server Update Service Vulnerability, CVE-2025-59287		https://www.cisa.gov/news-events/alerts/2025/10/24/microsoft-releases-out-band-security-update-mitigate-windows-server-update-service-vulnerability-cve
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-54236 Adobe Commerce and Magento Improper Input Validation Vulnerability ▪ CVE-2025-59287 Microsoft Windows Server Update Service (WSUS) Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2025/10/24/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
OpenAI Atlas Omnibox Is Vulnerable to Jailbreaks	https://www.securityweek.com/chatgpt-atlas-omnibox-is-vulnerable-to-jailbreaks/
$1M WhatsApp Hack Flops: Only Low-Risk Bugs Disclosed to Meta After Pwn2Own Withdrawal	https://www.securityweek.com/1m-whatsapp-hack-flops-only-low-risk-bugs-disclosed-to-meta-after-pwn2own-withdrawal/
Blitz Spear Phishing Campaign Targets NGOs Supporting Ukraine	https://www.infosecurity-magazine.com/news/blitz-spear-phishing-ngos-ukraine/
North Korean Hackers Attacking Unmanned Aerial Vehicle Industry to Steal Confidential Data	https://cybersecuritynews.com/north-korean-hackers-attacking-unmanned-aerial-vehicle-industry/
CISA Warns of Hackers Actively Exploiting Windows Server Update Services RCE Vulnerability in the Wild	https://cybersecuritynews.com/wsus-rce-vulnerability-exploited/

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
Medusa Ransomware Leaks 834 GB of Comcast Data After $1.2M Demand	https://hackread.com/medusa-ransomware-comcast-data-leak/?&web_view=true
Everest Ransomware Says It Stole 1.5M Dublin Airport Passenger Records	https://hackread.com/everest-ransomware-dublin-airport-passenger-data/

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
Newly Patched Critical Microsoft WSUS Flaw Comes Under Active Exploitation	https://thehackernews.com/2025/10/microsoft-issues-emergency-patch-for.html
Microsoft Issues Emergency Patch for Critical Windows Server Bug	https://www.darkreading.com/vulnerabilities-threats/microsoft-emergency-patch-windows-server-bug
Hackers launch mass attacks exploiting outdated WordPress plugins	https://www.bleepingcomputer.com/news/security/hackers-launch-mass-attacks-exploiting-outdated-wordpress-plugins/
Warlock Ransomware Actors Exploiting Sharepoint ToolShell Zero-Day Vulnerability in New Attack Wave	https://cybersecuritynews.com/warlock-ransomware-actors-exploiting-sharepoint-toolshell-zero-day/
Hackers Hijacking IIS Servers in The Wild Using Exposed ASP .NET Machine Keys to Inject Malicious Modules	https://cybersecuritynews.com/hackers-hijacking-iis-servers-in-the-wild/
WhatsApp 0-Click Vulnerability Privately Reported to Meta During Pwn2Own Hacking Contest	https://cybersecuritynews.com/whatsapp-exploit-privately-disclosed/

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

Potential threats / Threat intelligence

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

Σύντομη περιγραφή / Τίτλος	URL
New EDR-Redir Tool Breaks EDR Exploiting Bind Filter and Cloud Filter Driver	https://cybersecuritynews.com/edr-redir-tool-breaks-edr/
New CoPhish Attack Exploits Copilot Studio to Exfiltrate OAuth Tokens	https://cybersecuritynews.com/cophish-attack-exploits-copilot-studio/
706,000+ BIND 9 Resolver Instances Vulnerable to Cache Poisoning Exposed Online – PoC Released	https://cybersecuritynews.com/bind-9-resolver-instances/
LockBit 5.0 Actively Attacking Windows, Linux, and ESXi Environments	https://cybersecuritynews.com/lockbit-5-0-actively-attacking/
Hackers Weaponizing Telegram Messenger with Dangerous Android Malware to Gain Full System Control	https://cybersecuritynews.com/hackers-weaponizing-telegram-messenger/
Threat Actors Ramp Up Public App Exploits as ToolShell Gains Traction	https://www.infosecurity-magazine.com/news/toolshell-gains-traction/
Vault Viper Exploits Online Gambling Websites Using Custom Browser to Install Malicious Program	https://cybersecuritynews.com/vault-viper-exploits-online-gambling-websites/
Malicious NuGet Packages Mimic as Popular Nethereum Project to Steal Wallet Keys	https://cybersecuritynews.com/malicious-nuget-packages/
AI-Powered Ransomware Is the Emerging Threat That Could Bring Down Your Organization	https://cybersecuritynews.com/ai-powered-ransomware/
Decoding PIN-Protected BitLocker Through TPM SPI Analysis To Decrypt And Mount The Disks	https://cybersecuritynews.com/decoding-pin-protected-bitlocker/
New Caminho Malware Loader Uses LSB Steganography and to Hide .NET Payloads Within Image Files	https://cybersecuritynews.com/new-caminho-malware-loader-uses-lsb-steganography/

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/

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/