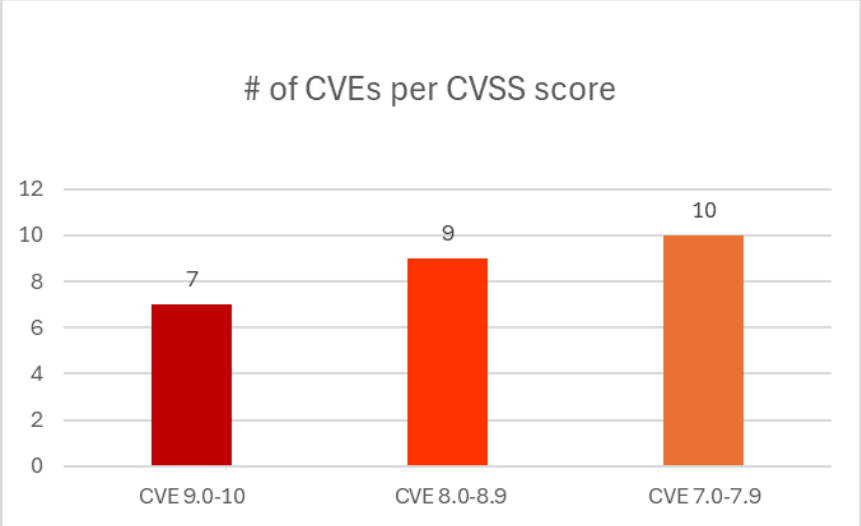
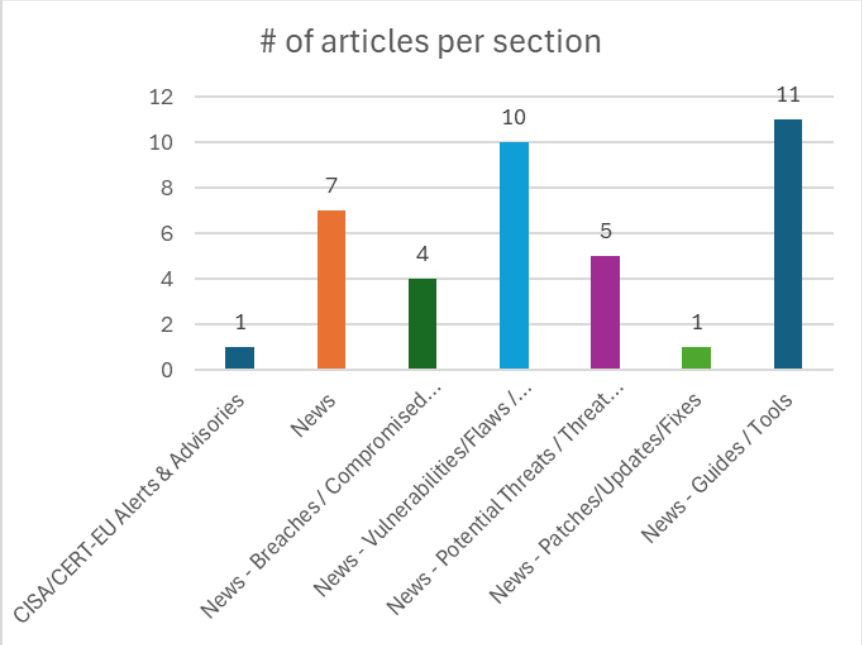
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 16/05/2026 - 19/05/2026





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)	CVSS v3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-42822	10,0	Microsoft Corporation	Improper Authentication	Improper authentication in Azure Local Disconnected Operations allows an unauthorized attacker to elevate privileges over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42822
https://nvd.nist.gov/vuln/detail/CVE-2018-25320	9,8	ACL Analytics	Improper Control of Generation of Code ('Code Injection')	11.x through 13.0.0.579	https://www.acl.com https://www.acl.com/products/acl-analytics/ https://www.exploit-db.com/exploits/44281 https://www.vulncheck.com/advisories/acl-analytics-11-x-arbitrary-code-execution
https://nvd.nist.gov/vuln/detail/CVE-2018-25332	9,8	GitBucket	Missing Authentication for Critical Function	4.23.1	https://github.com/gitbucket/gitbucket https://security.szurek.pl/ https://www.exploit-db.com/exploits/44668 https://www.vulncheck.com/advisories/gitbucket-unauthenticated-remote-code-execution
https://nvd.nist.gov/vuln/detail/CVE-2018-25335	9,8	WordPress Plugin Peugeot Music	Missing Authentication for Critical Function	1.0	https://www.exploit-db.com/exploits/44737 https://www.vulncheck.com/advisories/wordpress-plugin-peugeot-music-arbitrary-file-upload
https://nvd.nist.gov/vuln/detail/CVE-2020-37228	9,8	iDS6 DSSPro Digital Signage System	Improper Restriction of Excessive Authentication Attempts	6.2	http://www.yerootech.com https://www.exploit-db.com/exploits/48991 https://www.vulncheck.com/advisories/ids6-dsspro-digital-signage-system-captcha-security-bypass https://www.zeroscience.mk/en/vulnerabilities/ZSL-2020-5607.php
https://nvd.nist.gov/vuln/detail/CVE-2020-37239	9,8	libbabl	Double Free	0.1.62	https://www.exploit-db.com/exploits/49259 https://www.gegl.org https://www.gegl.org/babl/ https://www.vulncheck.com/advisories/libbabl-broken-double-free-detection-memory-safety
https://nvd.nist.gov/vuln/detail/CVE-2021-47952	9,8	python jsonpickle	Improper Control of Generation of Code ('Code Injection')	2.0.0	https://github.com/jsonpickle/jsonpickle https://jsonpickle.github.io https://www.exploit-db.com/exploits/49585 https://www.vulncheck.com/advisories/python-jsonpickle-remote-code-execution-via-py-repr
https://nvd.nist.gov/vuln/detail/CVE-2021-47976	8,8	TextPattern CMS	Cross-Site Request Forgery (CSRF)	4.9.0-dev	https://github.com/textpattern/textpattern https://textpattern.com/ https://www.exploit-db.com/exploits/50095 https://www.vulncheck.com/advisories/textpattern-

					cms-dev-authenticated-remote-code-execution-via-plugin-upload
https://nvd.nist.gov/vuln/detail/CVE-2026-45495	8,8	Microsoft Edge	Improper Input Validation	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45495
https://nvd.nist.gov/vuln/detail/CVE-2026-8719	8,8	The AI Engine – The Chatbot, AI Framework & MCP for WordPress	Improper Privilege Management	3.4.9	https://plugins.trac.wordpress.org/changeset/3533527/ai-engine https://www.wordfence.com/threat-intel/vulnerabilities/id/0593c20d-3422-4817-9639-614254b609db?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-8776	8,8	Edimax BR-6428NS	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1.10	https://lavender-bicycle-a5a.notion.site/EDIMAX-BR-6428NS-formPPTPSetup-34b53a41781f8074a88af068842b599e?source=copy_link https://vuldb.com/submit/811531 https://vuldb.com/vuln/364401 https://vuldb.com/vuln/364401/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-6346	8,7	Mattermost	Exposure of Sensitive Information to an Unauthorized Actor	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3	https://mattermost.com/security-updates
https://nvd.nist.gov/vuln/detail/CVE-2018-25330	8,2	Joomla! extension EkRishta	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2.10	https://extensions.joomla.org/extensions/extension/living/dating-a-relationships/ek-rishta/ https://www.exploit-db.com/exploits/44660 https://www.joomlaextensions.co.in/ https://www.vulncheck.com/advisories/joomla-ekrishta-persistent-xss-and-sql-injection
https://nvd.nist.gov/vuln/detail/CVE-2018-25333	8,2	Nordex N149/4.0-4.5 Wind Turbine Web Server	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	4.0	http://www.nordex-online.com https://www.exploit-db.com/exploits/44684 https://www.vulncheck.com/advisories/nordex-n149-wind-turbine-web-server-sql-injection
https://nvd.nist.gov/vuln/detail/CVE-2020-37243	8,2	Supsystic Pricing Table	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.8.7	https://downloads.wordpress.org/plugin/pricing-table-by-supsystic.1.8.7.zip https://supsystic.com/ https://www.exploit-db.com/exploits/49533 https://www.vulncheck.com/advisories/wordpress-plugin-supsystic-pricing-table-sql-injection-xss
https://nvd.nist.gov/vuln/detail/CVE-2026-46728	8,2	Das U-Boot	Origin Validation Error	2026.04	https://github.com/barebox/barebox/security/advisories/GHSA-3fvj-q26p-j6h4 https://github.com/u-boot/u-boot/commit/2092322b31cc8b1f8c9e2e238d1043ae0637b241
https://nvd.nist.gov/vuln/detail/CVE-2020-37232	7,8	Advanced System Care Service	Unquoted Search Path or Element	13.0.0.157	https://www.exploit-db.com/exploits/49049 https://www.iobit.com https://www.iobit.com/es/advancedsystemcarepro.php

					https://www.vulncheck.com/advisories/advanced-system-care-service-unquoted-service-path-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2021-47974	**7,8**	VX Search	Unquoted Search Path or Element	13.5.28	https://www.exploit-db.com/exploits/50026 https://www.vulncheck.com/advisories/vx-search-unquoted-service-path-privilege-escalation https://www.vxsearch.com
https://nvd.nist.gov/vuln/detail/CVE-2026-6347	**7,6**	Mattermost	Exposure of Sensitive Information to an Unauthorized Actor	attermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13, 11.4.x <= 11.4.3	https://mattermost.com/security-updates
https://nvd.nist.gov/vuln/detail/CVE-2021-47972	**7,5**	Sticky Notes & Color Widgets	Memory Allocation with Excessive Size Value	1.4.2	https://www.exploit-db.com/exploits/49957 https://www.vulncheck.com/advisories/sticky-notes-color-widgets-denial-of-service
https://nvd.nist.gov/vuln/detail/CVE-2021-47977	**7,5**	WordPress Plugin Anti-Malware Security and Bruteforce Firewall	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	4.20.59	https://gotmls.net/ https://gotmls.net/downloads/ https://www.exploit-db.com/exploits/50107 https://www.vulncheck.com/advisories/wordpress-anti-malware-security-bruteforce-firewall-directory-traversal
https://nvd.nist.gov/vuln/detail/CVE-2026-32323	**7,3**	Mullvad VPN	Improper Privilege Management	macOS with versions 2026.1 and below	https://github.com/mullvad/mullvadvpn-app/commit/032fdcb927c0b6d3e5e1aba4140d33adf22a6bfb https://github.com/mullvad/mullvadvpn-app/security/advisories/GHSA-c2g6-w5fq-vw3m
https://nvd.nist.gov/vuln/detail/CVE-2026-8725	**7,3**	CoreWorxLab CAAL	Server-Side Request Forgery (SSRF)	up to 1.6.0	https://github.com/juruo123/public_exp/issues/5 https://vuldb.com/submit/807753 https://vuldb.com/vuln/364316 https://vuldb.com/vuln/364316/cti
https://nvd.nist.gov/vuln/detail/CVE-2021-47975	**7,2**	WP Learn Manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	1.1.2	https://wordpress.org/plugins/learn-manager/ https://wplearnmanager.com/ https://www.exploit-db.com/exploits/50086 https://www.vulncheck.com/advisories/wordpress-plugin-wp-learn-manager-stored-xss
https://nvd.nist.gov/vuln/detail/CVE-2026-8764	**7,2**	H3C Magic B3	Improper Restriction of Operations within the Bounds of a Memory Buffer	up to 100R002	https://github.com/yyyy0031/CVE/issues/1 https://vuldb.com/submit/811373 https://vuldb.com/vuln/364389 https://vuldb.com/vuln/364389/cti
https://nvd.nist.gov/vuln/detail/CVE-2021-47980	**7,1**	Fuel CMS	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.4.13	https://github.com/daylightstudio/FUEL-CMS/archive/1.4.13.zip https://www.exploit-db.com/exploits/50523 https://www.getfuelcms.com/ https://www.vulncheck.com/advisories/fuel-cms-blind-sql-injection-via-col-parameter

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 One Known Exploited Vulnerability to Catalog	▪ CVE-2026-42897 Microsoft Exchange Server Cross-Site Scripting Vulnerability	https://www.cisa.gov/news-events/alerts/2026/05/15/cisa-adds-one-known-exploited-vulnerability-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
Can Laws Stop Deepfakes? South Korea Aims to Find Out	https://www.darkreading.com/vulnerabilities-threats/can-laws-stop-deepfakes-south-korea
Microsoft rejects critical Azure vulnerability report, no CVE issued	https://www.bleepingcomputer.com/news/security/microsoft-rejects-critical-azure-vulnerability-report-no-cve-issued/
Mythos Preview Builds PoC Exploits in Automated Vulnerability Research	https://cybersecuritynews.com/mythos-preview-builds-poc-exploits/
Linus Torvalds Says AI Bug Reports Have Made Linux Security Mailing List Unmanageable	https://cybersecuritynews.com/linus-torvalds-on-ai-bug-reports/
CISA Warns of Microsoft Exchange Server Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-microsoft-exchange-server-vulnerability/
Microsoft Confirms Windows 11 Update Fails With Error 0x800f0922	https://cybersecuritynews.com/microsoft-windows-11-update/
Fast16 Malware Manipulated Nuclear Weapons Simulation Data to Sabotage Test Results	https://cybersecuritynews.com/fast16-malware-manipulated-nuclear-weapons/

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**
Grafana Labs Security Breach – Hackers Access GitHub and Download Codebase	https://cybersecuritynews.com/grafana-labs-security-breach/
JDownloader Website Compromised to Distribute Malicious Windows and Linux Installers	https://cybersecuritynews.com/jdownloader-website-compromised/
Hackers Abuse Microsoft Entra ID Accounts to Exfiltrate Microsoft 365 and Azure Data	https://cybersecuritynews.com/hackers-abuse-microsoft-entra-id-accounts/
Hackers Actively Exploiting Critical NGINX RCE Vulnerability in the Wild	https://cybersecuritynews.com/hackers-exploiting-nginx-rce-vulnerability/

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
New Windows ‘MiniPlasma’ Zero-Day Let Attackers Gain SYSTEM Access – PoC Released	https://cybersecuritynews.com/windows-miniplasma-zero-day/
Critical WordPress Plugin Vulnerability Exposes Websites to Authentication Bypass Attacks	https://cybersecuritynews.com/wordpress-plugin-vulnerability-exposes-websites/
Claude Code RCE Flaw Lets Attackers Execute Commands via Malicious Deeplinks	https://cybersecuritynews.com/claude-code-rce-flaw/
Critical Linux Kernel Flaw ‘ssh-keysign-pwn’ Exposes SSH Keys and Shadow Passwords	https://cybersecuritynews.com/linux-kernel-vulnerability-ssh-keysign-pwn/
Malicious JPEG Images Could Trigger PHP Memory Safety Vulnerabilities	https://cybersecuritynews.com/malicious-jpeg-images-php-memory-safety-vulnerabilities/
Microsoft Exchange, Windows 11, and Cursor Zero-Days Exploited on Pwn2Own Day 2	https://cybersecuritynews.com/microsoft-exchange-windows-11-and-cursor-zero-days-exploited-pwn2own/
PoC Code Published for Critical NGINX Vulnerability	https://www.securityweek.com/poc-code-published-for-critical-nginx-vulnerability/
Funnel Builder Flaw Under Active Exploitation Enables WooCommerce Checkout Skimming	https://thehackernews.com/2026/05/funnel-builder-flaw-under-active.html
Critical n8n Vulnerabilities Expose Automation Nodes to Full RCE	https://cybersecuritynews.com/n8n-rce-vulnerabilities/
New Windows ‘MiniPlasma’ Zero-Day Let Attackers Gain SYSTEM Access – PoC Released	https://cybersecuritynews.com/windows-miniplasma-zero-day/

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 Confirms Windows 11 Update Fails With Error 0x800f0922	https://cybersecuritynews.com/microsoft-windows-11-update/

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
Fast16 Malware Manipulated Nuclear Weapons Simulation Data to Sabotage Test Results	https://cybersecuritynews.com/fast16-malware-manipulated-nuclear-weapons/
Google Project Zero Discloses Zero-Click Exploit Chain for Pixel 10 Devices	https://cybersecuritynews.com/zero-click-exploit-chain-pixel-10-devices/
Four Malicious npm Packages Steal SSH Keys, Cloud Credentials, and Crypto Wallets	https://cybersecuritynews.com/malicious-npm-packages-steal-keys/
1 Million WordPress Sites Affected by Avada Builder File Read and SQL Injection Flaws	https://cybersecuritynews.com/avada-builder-plugin-vulnerability/
Critical WordPress Plugin Vulnerability Exposes Websites to Authentication Bypass Attacks	https://cybersecuritynews.com/wordpress-plugin-vulnerability-exposes-websites/

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/