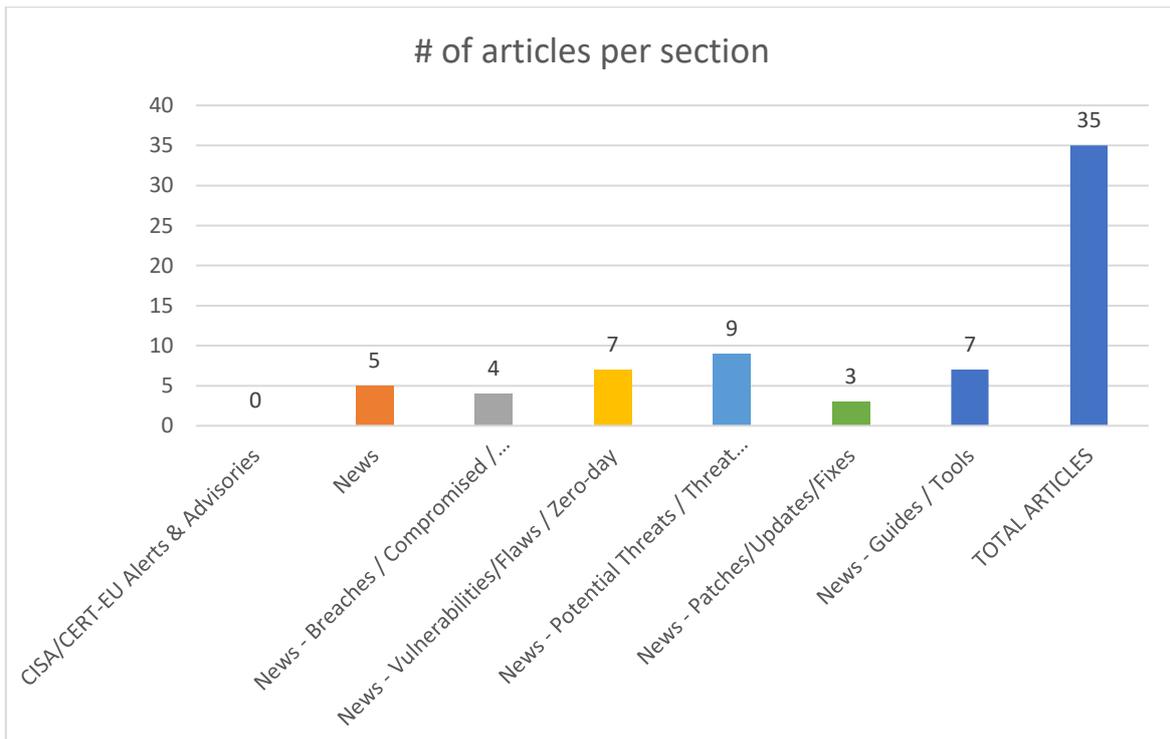
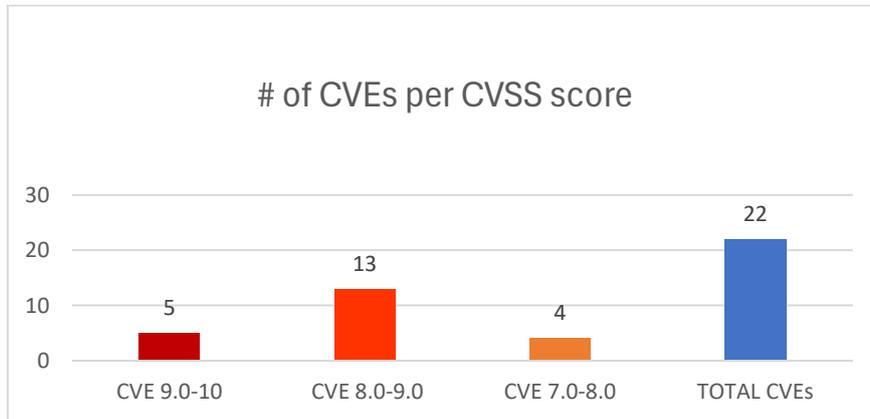




Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 31/01/2026 - 03/02/2026



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories	7
News.....	7
Breaches / Compromised / Hacked.....	8
Vulnerabilities / Flaws / Zero-day.....	8
Patches / Updates / Fixes	9
Potential threats / Threat intelligence	9
Guides / Tools.....	10
References.....	11
Annex - Websites with vendor specific vulnerabilities.....	12

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-2020-37052	9,8	AirControl	Improper Control of Generation of Code ('Code Injection')	1.4.2	https://www.exploit-db.com/exploits/48541 VulnCheck https://www.ui.com/VulnCheck https://www.vulncheck.com/advisories/aircontrol-preauth-remote-code-execution
https://nvd.nist.gov/vuln/detail/CVE-2020-37050	9,8	Quick Player	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1.3	https://download.cnet.com/quick-player/3000-2168_4-10871417.html VulnCheck https://web.archive.org/web/20201022211753/https://whitecr0wz.github.io/posts/Exploiting-Quick-Player/ VulnCheck https://web.archive.org/web/20210105222205/https://whitecr0wz.github.io/assets/img/Findings6/18.gif VulnCheck https://www.exploit-db.com/exploits/48564 VulnCheck https://www.vulncheck.com/advisories/quick-player-ml-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2020-37043	9,8	10-Strike Bandwidth Monitor	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	3.9	https://www.10-strike.com/bandwidth-monitor/ VulnCheck https://www.exploit-db.com/exploits/48570 VulnCheck https://www.vulncheck.com/advisories/strike-bandwidth-monitor-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2020-37027	9,8	Sickbeard alpha	Improper Neutralization of Special Elements used in an OS		https://github.com/midgetspy/Sick-Beard VulnCheck https://web.archive.org/web/20190722085652/https://sickbeard.com/ VulnCheck https://www.exploit-db.com/exploits/48646 VulnCheck

			Command ('OS Command Injection')		https://www.vulncheck.com/advisories/sickbeard-remote-command-injection
https://nvd.nist.gov/vuln/detail/CVE-2019-25232	9,8	NetPCLinker	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1.0.0.0	https://sourceforge.net/projects/netpclinker/ VulnCheck https://www.exploit-db.com/exploits/48680 VulnCheck https://www.vulncheck.com/advisories/netpclinker-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2020-37057	8,8	Online-Exam-System 2015	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://github.com/sunnygkp10/Online-Exam-System-.git VulnCheck https://www.exploit-db.com/exploits/48529 VulnCheck https://www.vulncheck.com/advisories/online-exam-system-fid-sql-injection
https://nvd.nist.gov/vuln/detail/CVE-2020-37023	8,8	Koken CMS	Unrestricted Upload of File with Dangerous Type	0.22.24	http://koken.me/ VulnCheck https://github.com/V1n1v131r4/Bypass-File-Upload-on-Koken-CMS/blob/master/README.md VulnCheck https://www.exploit-db.com/exploits/48706 VulnCheck https://www.softaculous.com/apps/cms/Koken VulnCheck https://www.vulncheck.com/advisories/koken-cms-arbitrary-file-upload
https://nvd.nist.gov/vuln/detail/CVE-2020-37049	8,4	Frigate	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	3.36.0.9	https://web.archive.org/web/20190623044943/http://www.frigate3.com/index.php VulnCheck https://www.exploit-db.com/exploits/48563 VulnCheck https://www.vulncheck.com/advisories/frigate-command-line-local-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2020-37040	8,4	Code Blocks	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17.12	http://www.codeblocks.org/ VulnCheck https://sourceforge.net/projects/codeblocks/ VulnCheck https://www.exploit-db.com/exploits/48594 VulnCheck https://www.vulncheck.com/advisories/code-blocks-file-name-local-buffer-overflow

https://nvd.nist.gov/vuln/detail/CVE-2020-37036	8,4	RM Downloader	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2.50.60	https://github.com/x00x00x00x00/RMDownloader_2.50.60 VulnCheck https://rm-downloader.software.informer.com/VulnCheck https://www.exploit-db.com/exploits/48628 VulnCheck https://www.vulncheck.com/advisories/rm-downloader-load-local-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2020-37036	8,4	RM Downloader	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2.50.60	https://github.com/x00x00x00x00/RMDownloader_2.50.60 VulnCheck https://rm-downloader.software.informer.com/VulnCheck https://www.exploit-db.com/exploits/48628 VulnCheck https://www.vulncheck.com/advisories/rm-downloader-load-local-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2020-37028	8,4	Socusoft Photo to Video Converter Professional	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	8.07	https://web.archive.org/web/20190314225058/http://www.dvd-photo-slideshow.com/photo-to-video-converter.html VulnCheck https://www.exploit-db.com/exploits/48691 VulnCheck https://www.vulncheck.com/advisories/socusoft-photo-to-video-converter-professional-output-folder-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2020-37029	8,4	FTPDummy	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	4.80	http://www.dummysoftware.com/ftpdummy.html VulnCheck https://www.exploit-db.com/exploits/48685 VulnCheck https://www.vulncheck.com/advisories/ftpdummy-local-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2020-37031	8,4	Simple Startup Manager	Out-of-bounds Write	1.17	https://www.ashkon.com/startup_manager.html VulnCheck https://www.exploit-db.com/exploits/48678 VulnCheck https://www.vulncheck.com/advisories/simple-startup-manager-file-local-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2020-37024	8,4	Nidesoft DVD Ripper	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	5.2.18	https://nidesoft-dvd-ripper.softonic.com/ VulnCheck https://www.exploit-db.com/exploits/48687 VulnCheck https://www.vulncheck.com/advisories/nidesoft-dvd-ripper-local-buffer-overflow
https://nvd.nist.gov/vuln/detail/CVE-2025-36384	8,4	IBM Db2 for Windows	Unquoted Search Path or Element	12.1.0 - 12.1.3	https://www.ibm.com/support/pages/node/7257678

https://nvd.nist.gov/vuln/detail/CVE-2020-37035	8,2	e-Learning PHP Script	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0.1.0	https://github.com/amitkolloldey/elearning-script VulnCheck https://www.exploit-db.com/exploits/48629 VulnCheck https://www.vulncheck.com/advisories/e-learning-php-script-search-sql-injection
https://nvd.nist.gov/vuln/detail/CVE-2020-37033	8,2	Infor Storefront B2B	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://web.archive.org/web/20191223051205/https://www.insitesoft.com/infor-storefront/ VulnCheck https://www.exploit-db.com/exploits/48674 VulnCheck https://www.vulncheck.com/advisories/infor-storefront-bb-username-sql-injection
https://nvd.nist.gov/vuln/detail/CVE-2026-25153	7,7	Backstage	Improper Control of Generation of Code ('Code Injection')	prior to 1.13.11 and 1.14.1	https://github.com/backstage/backstage/security/advisories/GHSA-6jr7-99pf-8vgf
https://nvd.nist.gov/vuln/detail/CVE-2020-37041	7,5	OpenCTI	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	3.3.1	https://github.com/OpenCTI-Platform/opencti VulnCheck https://www.exploit-db.com/exploits/48595 VulnCheck https://www.opencti.io/ VulnCheck https://www.vulncheck.com/advisories/opencti-directory-traversal
https://nvd.nist.gov/vuln/detail/CVE-2020-37034	7,5	HelloWeb	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	2.0	https://web.archive.org/web/20190109182037/https://helloworld.co.kr/ VulnCheck https://www.exploit-db.com/exploits/48659 VulnCheck https://www.vulncheck.com/advisories/helloweb-arbitrary-file-download
https://nvd.nist.gov/vuln/detail/CVE-2026-25156	7,3	HotCRP	Improper Neutralization of Input During Web Page Generation		https://github.com/kohler/hotcrp/commit/8933e86c9f384b356dc4c6e9e2814dee1074b323 GitHub, Inc. https://github.com/kohler/hotcrp/commit/aa20ef288828b04550950cf67c831af8a525f508 GitHub,

			('Cross-site Scripting')		Inc. https://github.com/kohler/hotcrp/commit/c3d88a7e18d52119c65df31c2cc994edd2beccc5 GitHub, Inc. https://github.com/kohler/hotcrp/security/advisories/GHSA-p88p-2f2p-2476
--	--	--	--------------------------	--	--

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

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
30 Wind and Solar Farms in Poland Faced Coordinated Cyberattacks	https://cybersecuritynews.com/solar-farms-in-poland-faced-coordinated-cyberattacks/
Russian Hacker Alliance Targeting Denmark in Large-Scale Cyberattack	https://cybersecuritynews.com/russian-hacker-alliance-targeting-denmark/
Former Google Engineer Found Guilty of Stealing AI Secrets	https://www.infosecurity-magazine.com/news/former-google-engineer-guilty/
NSA Publishes New Zero Trust Implementation Guidelines	https://www.infosecurity-magazine.com/news/nsa-zero-trust-implementation/
Weekly Recap: Proxy Botnet, Office Zero-Day, MongoDB Ransoms, AI Hijacks & New Threats	https://thehackernews.com/2026/02/weekly-recap-proxy-botnet-office-zero.html

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
Hackers Attacking MongoDB Instances to Delete Database and Add Ransom Note	https://cybersecuritynews.com/mongodb-instances-hacked/
California tribal clinics warn patients of data breach that leaked SSNs and medical info	https://www.comparitech.com/news/california-tribal-clinics-warn-patients-of-data-breach-that-leaked-ssns-and-medical-info/?web_view=true
CrossCurve Bridge Hacked for \$3M After Smart Contract Validation Vulnerability Exploited	https://thecyberexpress.com/crosscurve-bridge-3m-cyberattack/?web_view=true
ShinyHunters swipes right on 10M records in alleged dating app data grab	https://www.theregister.com/2026/01/29/shinyhunters_match_group/?web_view=true

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
Hackers Exploiting Microsoft Office 0-day Vulnerability to Deploy Malware	https://cybersecuritynews.com/microsoft-office-0-day-vulnerability-exploited/
Gakido CRLF Injection Vulnerability Let Attackers Bypass Security Controls	https://cybersecuritynews.com/gakido-crlf-injection-vulnerability/
1-Click Clawdbot Vulnerability Enable Malicious Remote Code Execution Attacks	https://cybersecuritynews.com/1-click-clawdbot-vulnerability-enable-malicious-remote-code-execution-attacks/
Notepad++ Update Servers Hijacked to Redirect Users to Malicious Servers	https://cybersecuritynews.com/notepad-hijacked/
Critical Johnson Controls Products Vulnerabilities Enables Remote SQL Injection Attacks	https://cybersecuritynews.com/johnson-controls-products-vulnerabilities/
Moltbook AI Vulnerability Exposes Email Addresses, Login Tokens, and API Keys	https://cybersecuritynews.com/moltbook-ai-vulnerability/
SCADA Vulnerability Triggers DoS, Potentially Disrupting Industrial Operations	https://cybersecuritynews.com/scada-vulnerability-triggers-dos/

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
Metasploit Releases 7 New Exploit Modules covering FreePBX, Cacti and Smarter-Mail	https://cybersecuritynews.com/metasploit-exploit-modules/
Ivanti Patches Exploited EPMM Zero-Days	https://www.securityweek.com/ivanti-patches-exploited-epmm-zero-days/
SmarterMail Fixes Critical Unauthenticated RCE Flaw with CVSS 9.3 Score	https://thehackernews.com/2026/01/smartermail-fixes-critical.html

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
OpenClaw AI Agent Skills Abused by Threat Actors to Deliver Malware	https://cybersecuritynews.com/openclaw-ai-agent-skills-abused/
Notepad++ Hack Detailed Along With the IoCs and Custom Malware Used	https://cybersecuritynews.com/notepad-hack/
DynoWiper Data-Wiping Malware Attacking Energy Companies to Destroy Data	https://cybersecuritynews.com/dynowiper-data-wiping-malware/
New Punishing Owl Hacker Group Targeting Networks of Russian Government Security Agency	https://cybersecuritynews.com/new-punishing-owl-hacker-group-targeting-networks/
Pulsar RAT Attacking Windows Systems via Per-user Run Registry Key and Exfiltrates Sensitive Details	https://cybersecuritynews.com/pulsar-rat-attacking-windows-systems/
New Stealthy Fileless Linux Malware 'ShadowHS' Emphasizes Automated Propagation	https://cybersecuritynews.com/new-stealthy-fileless-linux-malware-shadowhs/
Arsink Rat Attacking Android Devices to Exfiltrate Sensitive Data and Enable Remote Access	https://cybersecuritynews.com/arsink-rat-attacking-android-devices/
Windows 11 New Security Feature Denies Unauthorized Access to System Files	https://cybersecuritynews.com/windows-11-new-security-feature/
Fancy Bear Exploits Microsoft Office Flaw in Ukraine, EU Cyber-Attacks	https://www.infosecurity-magazine.com/news/fancy-bear-exploits-office-flaw/

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

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/