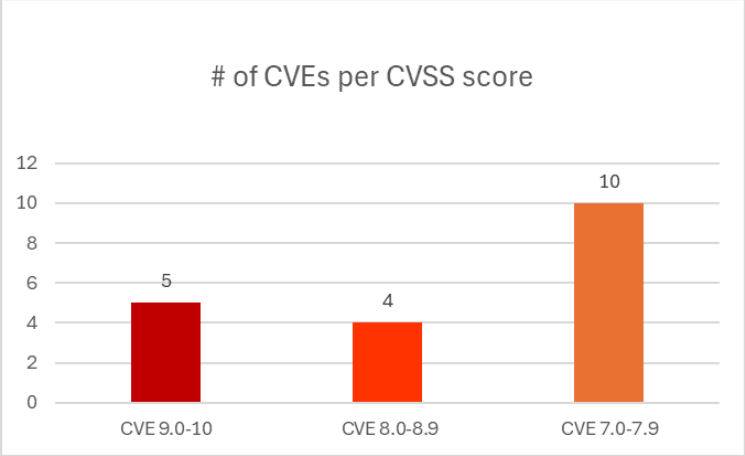
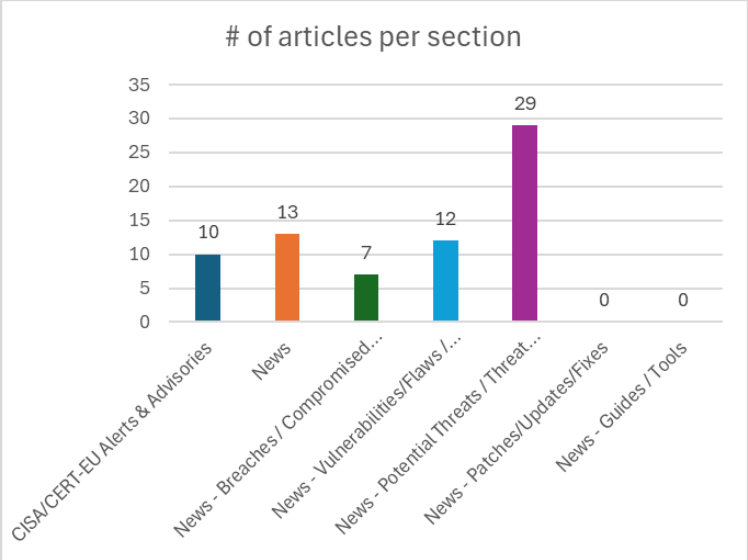
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 02/09/2025 - 05/09/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

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-2025-53693	9,8	Sitecore Experience	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	Sitecore Experience Manager (XM): from 9.0 through 9.3, from 10.0 through 10.4; Experience Platform (XP): from 9.0 through 9.3, from 10.0 through 10.4	https://labs.watchtowr.com/cache-me-if-you-can-sitecore-experience-platform-cache-poisoning-to-rce/ https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003667
https://nvd.nist.gov/vuln/detail/CVE-2025-57052	9,8	cJSON	Out-of-bounds Read	cJSON 1.5.0 through 1.7.18	https://x-0r.com/posts/cJSON-Array-Index-Parsing-Vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2025-57140	9,8	rsbi-pom	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	rsbi-pom 4.7	https://github.com/line2222/vuln/issues/5 https://github.com/ruisibi/rsbi-pom
https://nvd.nist.gov/vuln/detail/CVE-2025-56752	9,4	Ruijie	Improper Authentication	Ruijie RG-ES series switch firmware ESW_1.0(1)B1P39	https://github.com/TNCX-byte/Vulnerability_Research/blob/main/CVE-2025-56752/README.md
https://nvd.nist.gov/vuln/detail/CVE-2025-53690	9,0	Sitecore Experience	Deserialization of Untrusted Data	Sitecore Experience Manager (XM), Sitecore Experience Platform (XP)	https://cloud.google.com/blog/topics/threat-intelligence/viewstate-deserialization-zero-day-vulnerability https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865
https://nvd.nist.gov/vuln/detail/CVE-2025-9812	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CH22 1.0.0.1	https://github.com/csgii/cve/issues/1 https://vuldb.com/?ctiid.322139 https://vuldb.com/?id.322139 https://vuldb.com/?submit.641148 https://www.tenda.com.cn/

https://nvd.nist.gov/vuln/detail/CVE-2025-9864	8,8	V8 in Google Chrome	Use After Free	V8 in Google Chrome prior to 140.0.7339.80	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/434513380
https://nvd.nist.gov/vuln/detail/CVE-2025-9866	8,8	Extensions in Google Chrome	Protection Mechanism Failure	Extensions in Google Chrome prior to 140.0.7339.80	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/379337758
https://nvd.nist.gov/vuln/detail/CVE-2025-2413	8,6	Akinsoft	Improper Restriction of Excessive Authentication Attempts	Akinsoft ProKuafor: from s1.02.08 before v1.02.08	https://www.usom.gov.tr/bildirim/tr-25-0204
https://nvd.nist.gov/vuln/detail/CVE-2025-9365	7,8	Fuji Electric	Deserialization of Untrusted Data	Fuji Electric FRENIC-Loader 4	https://felib.fujielectric.co.jp/en/M10009/M20029/document_detail/b2f23970-e560-4961-8013-fc72be43681a https://www.cisa.gov/news-events/ics-advisories/icsa-25-245-02
https://nvd.nist.gov/vuln/detail/CVE-2025-9784	7,8	Undertow	Improper Resource Shutdown or Release		https://access.redhat.com/security/cve/CVE-2025-9784 https://bugzilla.redhat.com/show_bug.cgi?id=2392306
https://nvd.nist.gov/vuln/detail/CVE-2025-9815	7,8	alaneuler batteryKid up to 2.1 on macOS	Improper Authentication	alaneuler batteryKid up to 2.1 on macOS	https://github.com/SwayZGl1tZyyy/n-days/blob/main/batteryKid/README.md https://github.com/SwayZGl1tZyyy/n-days/blob/main/batteryKid/README.md#proof-of-concepts https://vuldb.com/?ctiid.322142 https://vuldb.com/?id.322142 https://vuldb.com/?submit.641358
https://nvd.nist.gov/vuln/detail/CVE-2025-9817	7,8	Wireshark	NULL Pointer Dereference	SSH dissector crash in Wireshark 4.4.0 to 4.4.8 allows denial of service	https://gitlab.com/wireshark/wireshark/-/issues/20642 https://www.wireshark.org/security/wnpa-sec-2025-03.html
https://nvd.nist.gov/vuln/detail/CVE-2025-58604	7,6	Mail Mint	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Mail Mint: from n/a through 1.18.5	https://patchstack.com/database/wordpress/plugin/mail-mint/vulnerability/wordpress-mail-mint-plugin-1-18-5-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9959	7,6	Python	Improper Control of Generation of Code ('Code Injection')	Incomplete validation of dunder attributes allows an attacker to escape from the Local Python execution en-	https://github.com/huggingface/smolagents/pull/1551 https://research.jfrog.com/vulnerabilities/smolagents-local-python-sandbox-escape-jfsa-2025-001434277/

				vironment sand-box, enforced by smolagents.	
https://nvd.nist.gov/vuln/detail/CVE-2025-52494	7,5	Adacore Ada Web Server (AWS)	Uncontrolled Resource Consumption	Adacore Ada Web Server (AWS) be-fore 25.2	https://adacore.com https://docs.adacore.com/corp/security-advisories/SEC.AWS-0095-v1.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-55852	7,5	Tenda	Stack-based Buffer Overflow	Tenda AC8 v16.03.34.06	https://github.com/CyberJ3ff/IOT/blob/main/tenda/tenda%20AC8%20v4%20V16.03.34.06/detail.md
https://nvd.nist.gov/vuln/detail/CVE-2025-41690	7,4	bluetooth	Insertion of Sensitive Infor-mation into Log File		https://certvde.com/en/advisories/VDE-2025-068
https://nvd.nist.gov/vuln/detail/CVE-2025-57833	7,1	Django	Improper Neu-tralization of Special Ele-ments used in an SQL Com-mand ('SQL In-jection')	Django 4.2 before 4.2.24, 5.1 before 5.1.12, and 5.2 be-fore 5.2.6	https://docs.djangoproject.com/en/dev/releases/security/ https://groups.google.com/g/django-announce https://www.djangoproject.com/weblog/2025/sep/03/security-releases/

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-38352 Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability ▪ CVE-2025-48543 Android Runtime Unspecified Vulnerability ▪ CVE-2025-53690 Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2025/09/04/cisa-adds-three-known-exploited-vulnerabilities-catalog
CISA Releases Five Industrial Control Systems Advisories	▪ ICSA-25-247-01 Honeywell OneWireless Wireless Device Manager (WDM) ▪ ICSA-25-217-01 Mitsubishi Electric Iconics Digital Solutions Multiple Products (Update A) ▪ ICSA-25-105-07 Delta Electronics COMMGR (Update A) ▪ ICSA-25-205-03 Honeywell Experion PKS (Update A) ▪ ICSA-25-191-10 End-of-Train and Head-of-Train Remote Linking Protocol (Update B)	https://www.cisa.gov/news-events/alerts/2025/09/04/cisa-releases-five-industrial-control-systems-advisories
Honeywell OneWireless Wireless Device Manager (WDM)		https://www.cisa.gov/news-events/ics-advisories/icsa-25-247-01
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2023-50224 TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability ▪ CVE-2025-9377 TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2025/09/03/cisa-adds-two-known-exploited-vulnerabilities-catalog

CISA, NSA, and Global Partners Release a Shared Vision of Software Bill of Materials (SBOM) Guidance		https://www.cisa.gov/news-events/alerts/2025/09/03/cisa-nsa-and-global-partners-release-shared-vision-software-bill-materials-sbom-guidance
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2020-24363 TP-link TL-WA855RE Missing Authentication for Critical Function Vulnerability ▪ CVE-2025-55177 Meta Platforms WhatsApp Incorrect Authorization Vulnerability	https://www.cisa.gov/news-events/alerts/2025/09/02/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Releases Four Industrial Control Systems Advisories	▪ ICSA-25-245-01 Delta Electronics EIP Builder ▪ ICSA-25-245-02 Fuji Electric FRENIC-Loader 4 ▪ ICSA-25-245-03 SunPower PVS6 ▪ ICSA-25-182-06 Hitachi Energy Relion 670/650 and SAM600-IO Series (Update A)	https://www.cisa.gov/news-events/alerts/2025/09/02/cisa-releases-four-industrial-control-systems-advisories
SunPower PVS6		https://www.cisa.gov/news-events/ics-advisories/icsa-25-245-03
Fuji Electric FRENIC-Loader 4	CVE-2025-9365	https://www.cisa.gov/news-events/ics-advisories/icsa-25-245-02
Delta Electronics EIP Builder		https://www.cisa.gov/news-events/ics-advisories/icsa-25-245-01

News

Σύντομη περιγραφή / Τίτλος	URL
Windows Heap-based Buffer Overflow Vulnerability Let Attackers Elevate Privileges	https://cybersecuritynews.com/windows-heap-based-buffer-overflow-vulnerability/
GhostRedirector Hackers Compromise Windows Servers With Malicious IIS Module To Manipulate Search Results	https://cybersecuritynews.com/ghostredirector-hacks-windows-servers/
Hackers Leverage X's Grok AI To Amplify Malicious Links Via Promoted Posts	https://cybersecuritynews.com/hackers-exploit-xs-grok-ai/
Google Services Down For Most Of The Users In US, Turkey And Eastern Europe	https://cybersecuritynews.com/google-down/
Microsoft Confirms UAC Bug Breaks App Install On Windows 11 And 10 Versions	https://cybersecuritynews.com/windows-uac-bug-breaks-app/
Mis-issued TLS Certificates for 1.1.1.1 DNS Service Enable Attackers to Decrypt Traffic	https://cybersecuritynews.com/tls-certificates-1-1-1-1-dns-service/
New 'NotDoor' Malware Attacks Outlook Users to Exfiltrate Data and Compromise Computers	https://cybersecuritynews.com/notdoor-malware-attack-outlook/
Attackers Are Abusing Malicious PDFs: Here's How to Spot Them Early	https://cybersecuritynews.com/attackers-are-abusing-malicious-pdfs-heres-how-to-spot-them-early/
AI-Powered Cybersecurity Tools Can Be Turned Against Themselves Through Prompt Injection Attacks	https://cybersecuritynews.com/ai-powered-tools-turned-against-themselves/
How IOC Feeds Streamline Incident Response and Threat Hunting for Best SOC Teams	https://cybersecuritynews.com/how-ioc-feeds-streamline-response-and-threat-hunting/
Microsoft to Kill Popular Editor Browser Extensions on Edge and Chrome	https://cybersecuritynews.com/microsoft-to-kill-poplar-editor-browser-extensions/
Record-breaking 11.5 Tbps UDP Flood DDoS Attack Originated from Google Cloud Platform	https://cybersecuritynews.com/record-breaking-ddos-attack-11-5-tbps/
28 Years of Nmap – From Simple Port Scanner to Comprehensive Network Security Suite	https://cybersecuritynews.com/28-years-of-nmap/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Chess.com Data Breach – Hackers Breached External System and Gained Internal Access	https://cybersecuritynews.com/chess-com-data-breach/
Bridgestone Confirms Cyberattack Impacts Manufacturing Facilities	https://cybersecuritynews.com/bridgestone-cyberattack/
Zscaler Confirms Data Breach – Hackers Compromised Salesforce Instance and Stole Customer Data	https://cybersecuritynews.com/zscaler-confirms-data-breach/
PagerDuty Confirms Data Breach After Third-Party App Vulnerability Exposes Salesforce Data	https://cybersecuritynews.com/pagerduty-confirms-data-breach/
Cloudflare Confirms Data Breach, Hackers Stole Customer Data from Salesforce Instances	https://cybersecuritynews.com/cloudflare-confirms-data-breach/
Jaguar Land Rover Confirms Cybersecurity Incident Impacts Global IT Systems	https://cybersecuritynews.com/jaguar-land-rover-it-systems/
Palo Alto Networks Confirms Data Breach – Hackers Stole Customer Data from Salesforce Instances	https://cybersecuritynews.com/palo-alto-networks-data-breach/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Hackers Scanning Cisco ASA Devices to Exploit Vulnerabilities from 25,000 Ips	https://cybersecuritynews.com/hackers-scanning-cisco-asa-devices-to-exploit-vulnerabilities-from-25000-ips/
Django Critical Vulnerability Let attackers Execute Malicious SQL Code on Web Servers	https://cybersecuritynews.com/django-sql-injection-vulnerability/
US Offers $10M Bounty For FSB Hackers Who Exploited Cisco Vulnerability To Attack Critical Infrastructure	https://cybersecuritynews.com/us-offers-10m-bounty-for-fsb-hackers/
Google Warns of Zero-Day Vulnerability in Sitecore Products Allowing Remote Code Execution	https://cybersecuritynews.com/sitecore-zero-day-vulnerability/
CISA Warns of Critical SunPower Device Vulnerability Let Attackers Gain Full Device Access	https://cybersecuritynews.com/cisa-warns-of-critical-sunpower-device-vulnerability/
Chrome Security Update – Patch for Vulnerabilities that Enable RCE Attacks	https://cybersecuritynews.com/chrome-140-released/
Android Security Update – Patch for 0-Day Vulnerabilities Actively Exploited in Attack	https://cybersecuritynews.com/android-security-update/
CISA Warns of WhatsApp 0-Day Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-whatsapp-0-day-vulnerability/
PoC Exploit Released for IIS WebDeploy Remote Code Execution Vulnerability	https://cybersecuritynews.com/poc-exploit-iis-vulnerability/
Hackers Leverage Hexstrike-AI Tool to Exploit Zero Day Vulnerabilities Within 10 Minutes	https://cybersecuritynews.com/hackers-leverage-hexstrike-ai-tool/
HashiCorp Vault Vulnerability Let Attackers to Crash Servers	https://cybersecuritynews.com/hashicorp-vault-vulnerability/
MobSF Security Testing Tool Vulnerability Let Attackers Upload Malicious Files	https://cybersecuritynews.com/mobsf-security-testing-tool-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Tycoon Phishing Kit Employs New Technique to Hide Malicious Links	https://cybersecuritynews.com/tycoon-phishing-kit-employs-new-technique/
NoisyBear Weaponizing ZIP Files to PowerShell Loaders and Exfiltrate Sensitive Data	https://cybersecuritynews.com/noisybear-weaponizing-zip-files/
Threat Actors Using Stealerium Malware to Attack Educational Organizations	https://cybersecuritynews.com/threat-actors-using-stealerium-malware/
Massive IPTV Hosted Across More Than 1,000 Domains and Over 10,000 IP Addresses	https://cybersecuritynews.com/massive-iptv-hosted-across-more-than-1000-domains/
Chinese APT Hackers Exploit Router Vulnerabilities to Infiltrate Enterprise Environments	https://cybersecuritynews.com/chinese-apt-hackers-exploit-router-vulnerabilities/
Threat Actors Attack PayPal Users in New Account Profile Set up Scam	https://cybersecuritynews.com/threat-actors-attack-paypal-users/
XWorm Malware With New Infection Chain Evade Detection Exploiting User and System Trust	https://cybersecuritynews.com/xworm-malware-with-new-infection-chain/
New Namespace Reuse Vulnerability Allows Remote Code Execution in Microsoft Azure AI, Google Vertex AI, and Hugging Face	https://cybersecuritynews.com/new-namespace-reuse-vulnerability/
1,100 Ollama AI Servers Exposed to Internet With 20% of Them are Vulnerable	https://cybersecuritynews.com/1100-ollama-ai-servers-exposed/
New Dire Wolf Ransomware Attack Windows Systems, Deletes Event Logs and Backup-Related Data	https://cybersecuritynews.com/new-dire-wolf-ransomware-attack-windows-systems/
Apache DolphinScheduler Default Permissions Vulnerability Fixed – Update Now	https://cybersecuritynews.com/apache-dolphinscheduler/
Google Won't Be Forced to Sell Chrome, But Must Share Search Data With Rivals	https://cybersecuritynews.com/google-wont-be-forced-to-sell-chrome/
MystRodX Leveraging DNS and ICMP to Steal Sensitive Data From Hacked Systems	https://cybersecuritynews.com/mystrodx-leveraging-dns-and-icmp/
Phishing Campaign Went Undetected for Over 3 Years on Google Cloud and Cloudflare	https://cybersecuritynews.com/phishing-campaign-went-undetected-for-over-3-years/
New Stealthy Python Malware Leverages Discord to Steal Data From Windows Machines	https://cybersecuritynews.com/new-stealthy-python-malware-leverages-discord/
RapperBot Hijacking Devices to Launch DDoS Attack In a Split Second	https://cybersecuritynews.com/rapperbot-hijacking-devices/
New TinyLoader Malware Attacking Windows Users Via Network Shares and Fake Shortcuts Files	https://cybersecuritynews.com/new-tinyloader-malware-attacking-windows-users/
ESPHome Web Server Authentication Bypass Vulnerability Exposes Smart Devices	https://cybersecuritynews.com/esphome-web-server-authentication-bypass/
Google Confirms That Claims of Major Gmail Security Warning are False	https://cybersecuritynews.com/gmail-security-warning-are-false/
New Phishing Attack Via OneDrive Attacking C-level Employees for Corporate Credentials	https://cybersecuritynews.com/new-phishing-attack-via-onedrive-attacking-c-level-employees/
New Report on Commercial Spyware Vendors Detailing Their Targets and Infection Chains	https://cybersecuritynews.com/new-report-on-commercial-spyware-vendors/
Iran-Nexus Hackers Abuses Omani Mailbox to Target Global Governments	https://cybersecuritynews.com/iran-nexus-hackers-abuses-omani-mailbox/
Ukrainian Networks Launch Massive Brute-Force and Password-Spraying Campaigns Targeting SSL VPN and RDP Systems	https://cybersecuritynews.com/ukrainian-networks-launch-massive-brute-force/

New WhatsApp Scam Alert Tricks Users to Get Complete Access to Your WhatsApp Chats	https://cybersecuritynews.com/new-whatsapp-scam-alert-tricks-users/
New ClickFix Attack Mimic as AnyDesk Leverages Windows Search to Drop MetaS-tealer	https://cybersecuritynews.com/new-clickfix-attack-mimic-as-anydesk/
Lazarus Hackers Deploying Three RATs on Compromised Systems Possibly Using 0-Day Vulnerability	https://cybersecuritynews.com/lazarus-hackers-deploying-three-rats/
New TinkyWinkey Stealthily Attacking Windows Systems With Advanced Keylogging Capabilities	https://cybersecuritynews.com/new-tinkywinkey-stealthily-attacking-windows-systems/
Critical Qualcomm Vulnerabilities Allow Attackers to Execute Arbitrary Code Re-motely	https://cybersecuritynews.com/critical-qualcomm-vulnerabilities/
Azure Active Directory Vulnerability Exposes Credentials and Enables Attackers to Deploy Malicious Apps	https://cybersecuritynews.com/azure-active-directory-vulnerability/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL

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.

[3]. Τα CVEs που αφορούν Wordpress plugins θα εμφανίζονται σε ξεχωριστή ενότητα (1.1) σε περιόδους που η εμφάνισή τους είναι ιδιαίτερα αυξημένη.

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/