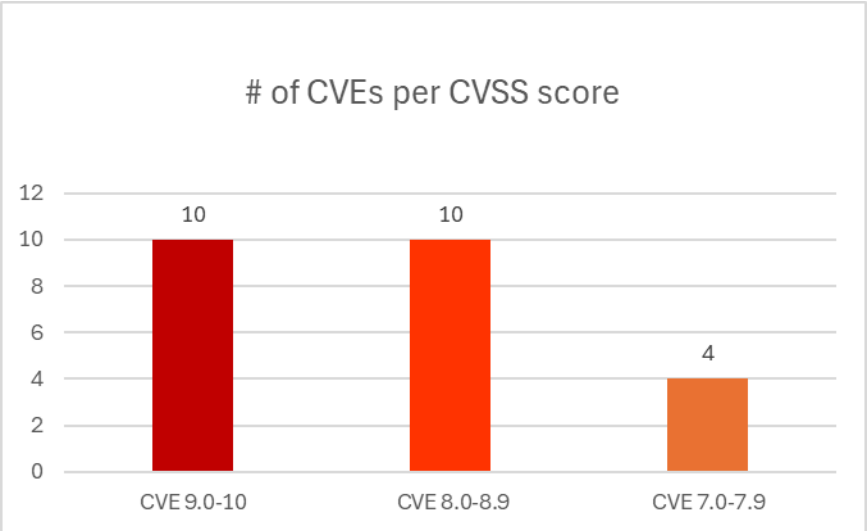
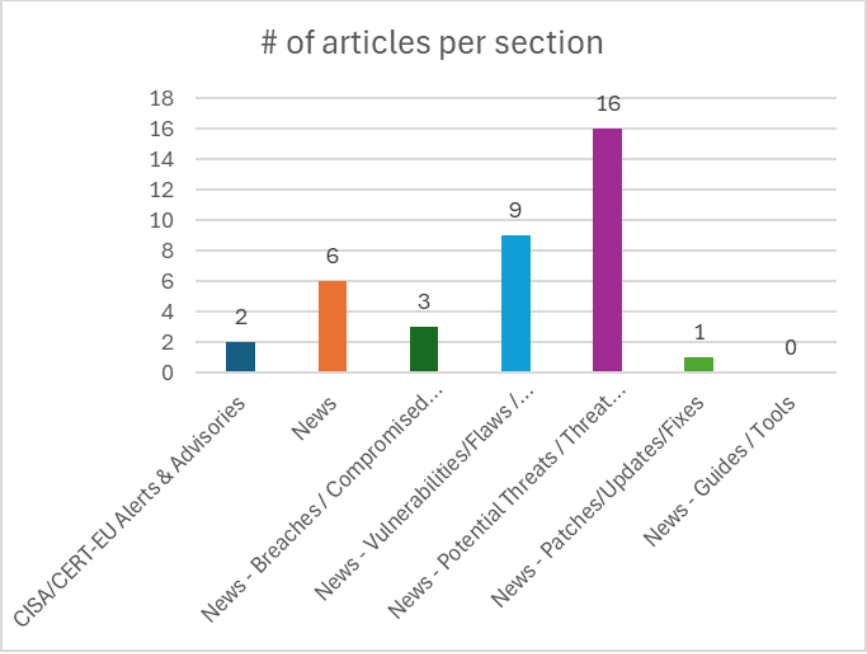
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 02/05/2026 - 05/05/2026





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-2026-42811	9,9	Apache Polaris	Improper Input Validation	-	http://www.openwall.com/lists/oss-security/2026/05/02/12 https://lists.apache.org/thread/hovn5hmkj9wj7v9cd8sn67svg03klgvg
https://nvd.nist.gov/vuln/detail/CVE-2026-42812	9,9	Apache Iceberg	Improper Input Validation	-	http://www.openwall.com/lists/oss-security/2026/05/02/13 https://lists.apache.org/thread/wxd2wj3p0smvrk84msv317wg5tp3jtw9
https://nvd.nist.gov/vuln/detail/CVE-2026-42370	9,8	GeoVision	Out-of-bounds Write	WebCam Server Login functionality of GeoVision GV-VMS V20 20.0.2	https://talosintelligence.com/vulnerability_reports/ https://www.geovision.com.tw/cyber_security.php
https://nvd.nist.gov/vuln/detail/CVE-2026-42373	9,8	D-Link	Use of Hard-coded Credentials	D-Link DIR-605L Hardware Revision B2 (End-of-Life, EOL)	https://www.securin.io/zero-day/cve-2026-42373-hardcoded-telnet-backdoor-in-d-link-dir-605l-b2-end-of-life-
https://nvd.nist.gov/vuln/detail/CVE-2026-42374	9,8	D-Link	Use of Hard-coded Credentials	D-Link DIR-600L Hardware Revision B1 (End-of-Life)	https://www.securin.io/zero-day/cve-2026-42374-hardcoded-telnet-backdoor-in-d-link-dir-600l-b1-end-of-life-
https://nvd.nist.gov/vuln/detail/CVE-2026-42375	9,8	D-Link	Use of Hard-coded Credentials	D-Link DIR-600L Hardware Revision A1 (End-of-Life)	https://www.securin.io/zero-day/cve-2026-42375-hardcoded-telnet-backdoor-in-d-link-dir-600l-a1-end-of-life-
https://nvd.nist.gov/vuln/detail/CVE-2026-42376	9,8	D-Link	Use of Hard-coded Credentials	D-Link DIR-456U Hardware Revision A1 (End-of-Life, EOL)	https://www.securin.io/zero-day/cve-2026-42376-hardcoded-telnet-backdoor-in-d-link-dir-456u-a1-end-of-life-
https://nvd.nist.gov/vuln/detail/CVE-2026-7719	9,8	Totolink	Improper Restriction of Operations within the Bounds of a Memory Buffer	Totolink WA300 5.2cu.7112_B20190227	https://lavender-bicycle-a5a.notion.site/TOTOLINK-WA300-loginAuth-34553a41781f8050b8ffc9e90a103cd5 https://vuldb.com/submit/807197 https://vuldb.com/vuln/360895 https://vuldb.com/vuln/360895/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-7747	9,8	Totolink	Improper Restriction of Operations within the Bounds of a Memory Buffer	Totolink N300RH 3.2.4-B20220812	https://lavender-bicycle-a5a.notion.site/TOTOLINK-N300RH-loginauth_password-34553a41781f80c0ad36f4d95122fd40?pvs=73 https://vuldb.com/submit/807201 https://vuldb.com/vuln/360922 https://vuldb.com/vuln/360922/cti https://www.totolink.net/

https://nvd.nist.gov/vuln/detail/CVE-2026-7823	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A8000RU 7.1cu.643_b20200521	https://github.com/Litengzheng/vuldb_new2/blob/main/A8000RU/vul_330/README.md https://vuldb.com/submit/807775 https://vuldb.com/vuln/361075 https://vuldb.com/vuln/361075/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-58074	8,8	Norton Secure VPN	Insecure Operation on Windows Junction / Mount Point	Norton Secure VPN via the Microsoft Store	https://talosintelligence.com/vulnerability_reports/TALOS-2025-2276 https://www.talosintelligence.com/vulnerability_reports/TALOS-2025-2276
https://nvd.nist.gov/vuln/detail/CVE-2026-23918	8,8	Apache HTTP Server	Double Free	Double Free and possible RCE vulnerability in Apache HTTP Server with the HTTP/2 protocol. This issue affects Apache HTTP Server: 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.	http://www.openwall.com/lists/oss-security/2026/05/04/19
https://nvd.nist.gov/vuln/detail/CVE-2026-24072	8,8	Apache HTTP Server	Improper Privilege Management	An escalation of privilege bug in various modules in Apache HTTP 2.4.66 and earlier allows local .htaccess authors to read files with the privileges of the httpd user. Users are recommended to upgrade to version 2.4.67, which fixes this issue.	http://www.openwall.com/lists/oss-security/2026/05/04/18 https://httpd.apache.org/security/vulnerabilities_24.html
https://nvd.nist.gov/vuln/detail/CVE-2026-42372	8,8	D-Link	Use of Hard-coded Credentials	D-Link DIR-605L Hardware Revision A1 (End-of-Life, EOL)	https://www.securin.io/zero-day/cve-2026-42372-hardcoded-telnet-backdoor-in-d-link-dir-605l-a1-end-of-life-
https://nvd.nist.gov/vuln/detail/CVE-2026-7675	8,8	Shenzhen Libituo Technology	Improper Restriction of Operations within the Bounds of a Memory Buffer	Shenzhen Libituo Technology LBT-T300-HW1 up to 1.2.8	https://github.com/hmKunlun/lbt-t300-hw1/blob/main/generate_conf_router(Channel).md https://vuldb.com/submit/800708 https://vuldb.com/submit/800709 https://vuldb.com/vuln/360828 https://vuldb.com/vuln/360828/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-7685	8,8	Edimax	Improper Restriction of Operations within the Bounds of a Memory Buffer	Edimax BR-6208AC up to 1.02	https://tzh00203.notion.site/Edimax-BR-6428nC-v1-16-setWAN-pptpDfGateway-Stack-Overflow-33db5c52018a80c1835dd4fab4b6c7f2 https://vuldb.com/submit/801606 https://vuldb.com/vuln/360844 https://vuldb.com/vuln/360844/cti

https://nvd.nist.gov/vuln/detail/CVE-2026-7717	8,8	Totolink	Improper Restriction of Operations within the Bounds of a Memory Buffer	Totolink WA300 5.2cu.7112_B20190227	https://lavender-bicycle-a5a.notion.site/TOTOLINK-WA300-UploadCustomModule-34553a41781f80a8a287e48a7fb04de9 https://vuldb.com/submit/807193 https://vuldb.com/vuln/360893 https://vuldb.com/vuln/360893/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-35228	8,7	Oracle MCP Server Helper Tool	-	The supported versions that is affected is 1.0.1-1.0.156	https://www.oracle.com/security-alerts/all-oracle-cves-outside-other-oracle-public-documents.html
https://nvd.nist.gov/vuln/detail/CVE-2026-42221	8,1	Nginx UI	Missing Authentication for Critical Function	Nginx UI is a web user interface for the Nginx web server. From version 2.0.0 to before version 2.3.8	https://github.com/0xJacky/nginx-ui/releases/tag/v2.3.8 https://github.com/0xJacky/nginx-ui/security/advisories/GHSA-h27v-ph7w-m9fp
https://nvd.nist.gov/vuln/detail/CVE-2026-42222	8,1	Nginx UI	Improper Access Control	Nginx UI is a web user interface for the Nginx web server. version 2.3.5	https://github.com/0xJacky/nginx-ui/security/advisories/GHSA-mxqh-q9h6-v8pq
https://nvd.nist.gov/vuln/detail/CVE-2026-34059	7,5	Apache HTTP Server	Buffer Over-read	Buffer Over-read vulnerability in Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.66. Users are recommended to upgrade to version 2.4.67, which fixes the issue.	http://www.openwall.com/lists/oss-security/2026/05/04/17 https://httpd.apache.org/security/vulnerabilities_24.html
https://nvd.nist.gov/vuln/detail/CVE-2026-42154	7,5	Prometheus	Uncontrolled Resource Consumption	Prometheus is an open-source monitoring system and time series database. Prior to versions 3.5.3 and 3.11.3	https://github.com/prometheus/prometheus/pull/18584 https://github.com/prometheus/prometheus/pull/18585 https://github.com/prometheus/prometheus/releases/tag/v3.11.3 https://github.com/prometheus/prometheus/releases/tag/v3.5.3 https://github.com/prometheus/prometheus/security/advisories/GHSA-8rm2-7qqf-34qm
https://nvd.nist.gov/vuln/detail/CVE-2026-7644	7,3	ChatGPTNextWeb NextChat	Incorrect Privilege Assignment	ChatGPTNextWeb NextChat up to 2.16.1	https://github.com/ChatGPTNextWeb/NextChat/ https://github.com/ChatGPTNextWeb/NextChat/issues/6757 https://vuldb.com/submit/806851 https://vuldb.com/vuln/360756 https://vuldb.com/vuln/360756/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-7736	7,3	GoBGP	Numeric Errors	osrg GoBGP up to 4.3.0	https://github.com/osrg/gobgp/ VulDB https://github.com/osrg/gobgp/commit/76d911046344a3923cbe573364197aa081944592 https://github.com/osrg/gobgp/releases/tag/v4.4.0 https://vuldb.com/submit/807604 https://vuldb.com/vuln/360911 https://vuldb.com/vuln/360911/cti

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
Careful Adoption of Agentic AI Services		https://www.cisa.gov/resources-tools/resources/careful-adoption-agentic-ai-services
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-31431 Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability	https://www.cisa.gov/news-events/alerts/2026/05/01/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
DOJ Sentences Two Americans to Prison for ALPHV BlackCat Attacks on U.S. Victims	https://cybersecuritynews.com/alphv-blackcat-attacks-on-u-s-victims/
Threat Actors Use AI to Automate 0-Day Discovery and Exploitation at Machine Speed	https://cybersecuritynews.com/threat-actors-use-ai-to-automate-0-day-discovery/
Ubuntu Website and Canonical Web Services Hit by DDoS Attack	https://cybersecuritynews.com/ubuntu-website-ddos-attack/
Ransomware Victims Jump to 7,831 as AI Crime Tools Scale Global Attacks	https://cybersecuritynews.com/ransomware-victims-jump-to-7831-as-ai-crime-tools/
Anthropic Launches Claude Security in Public Beta for Enterprise Customers	https://cybersecuritynews.com/claude-security-public-beta/
pnpm 11 Turns On Minimum Release Age by Default to Reduce npm Supply Chain Risk	https://cybersecuritynews.com/pnpm-11-turns-on-minimum-release-age/

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
DigiCert Hacked via Weaponized Screensaver File to Obtain EV Code Signing Certificates	https://cybersecuritynews.com/digicert-hacked-screensaver/
Trellix Source Code Breach – Hackers Gain Unauthorized Access to Repository	https://cybersecuritynews.com/trellix-source-code-breach/
Hackers Breach Government and Military Servers by Exploiting cPanel Vulnerability	https://cybersecuritynews.com/cpanel-vulnerability-exploited/

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
Microsoft Edge Stores All Saved Passwords in Cleartext Process Memory at Launch	https://cybersecuritynews.com/microsoft-edge-passwords-cleartext/
CISA Warns of Linux “Copy Fail” 0-Day Vulnerability Exploited to Root Systems	https://cybersecuritynews.com/linux-kernel-0-day-vulnerability-exploited/
Apache MINA Vulnerabilities Enables Remote Code Execution Attacks	https://cybersecuritynews.com/apache-mina-vulnerabilities/
CISA Warns of cPanel & WHM Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cpanel-whm-vulnerability-exploited/
Critical MOVEit Vulnerabilities Enables Authentication Bypass	https://cybersecuritynews.com/moveit-authentication-vulnerability/
FreeBSD DHCP Client Vulnerability Enables Remote Code Execution as Root	https://cybersecuritynews.com/freebsd-dhcp-client-vulnerability/
Microsoft Defender Mistakenly Flags DigiCert Root Certificates as Malware	https://cybersecuritynews.com/defender-flags-digicert-root-certificates/
Multiple Exim Mail Server Vulnerabilities Leads to Crash with Malicious DNS data	https://cybersecuritynews.com/exim-mail-server-vulnerabilities/
Critical Wireshark Vulnerabilities Let Attackers Execute Arbitrary Code Via Malformed Packets	https://cybersecuritynews.com/wireshark-vulnerabilities-code-execution/

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
Critical Apache HTTP Server Flaw Exposes Millions of Servers to RCE Attacks	https://cybersecuritynews.com/apache-http-server-rce/

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
New MicroStealer Malware Actively Attacking Telecom & Education Sectors	https://cybersecuritynews.com/new-microstealer-malware-actively-attacking/
Bluekit Phishing Kit Automates Domains, 2FA Lures, and Session Hijacking in One Panel	https://cybersecuritynews.com/bluekit-phishing-kit-automates-domains/
Malicious Tanstack Package Uses Postinstall Script to Steal Developer Environment Files	https://cybersecuritynews.com/malicious-tanstack-package-uses-postinstall-script/
New xlabs_v1 Botnet Targets Minecraft Servers Through ADB-Exposed Android Devices	https://cybersecuritynews.com/new-xlabs_v1-botnet-targets-minecraft-servers/
Attackers Weaponize SAP npm Packages to Steal GitHub, Cloud, and AI Coding Tool Secrets	https://cybersecuritynews.com/attackers-weaponize-sap-npm-packages/
Email Bombing and Fake IT Support Calls Fuel New Microsoft Teams Phishing Attacks	https://cybersecuritynews.com/email-bombing-and-fake-it-support-calls/
Attackers Deploy AiTM Phishing Pages to Access SharePoint, HubSpot, and Google Workspace	https://cybersecuritynews.com/attackers-deploy-aitm-phishing-page/
Attackers Abuse Google AppSheet, Netlify, and Telegram in Facebook Phishing Campaign	https://cybersecuritynews.com/attackers-abuse-google-appsheet-netlify-and-telegram/
cPanelSniper – PoC Exploit Disclosed for cPanel Vulnerability, 44,000 Servers Compromised	https://cybersecuritynews.com/cpanelsniper-poc-exploit/
EtherRAT Campaign Uses SEO Poisoning and GitHub Facades to Target Enterprise Admins	https://cybersecuritynews.com/etherrat-campaign-uses-seo-poisoning/
New Spyware Platform Lets Buyers Rebrand and Resell Android Surveillance Malware	https://cybersecuritynews.com/new-spyware-platform-lets-buyers-rebrand/
Attackers Abuse CAPTCHA and ClickFix Tactics to Boost Credential Theft Campaigns	https://cybersecuritynews.com/attackers-abuse-captcha-and-clickfix-tactics/
New DDoS Malware Exploits Jenkins to Attack Valve Source Engine Game Servers	https://cybersecuritynews.com/new-ddos-malware-exploits-jenkins/
Deep#Door Stealer Harvests Browser Passwords, Cloud Tokens, SSH Keys, and Wi-Fi Credentials	https://cybersecuritynews.com/deepdoor-stealer-harvests-browser-passwords/
China-Aligned Attackers Use ShadowPad, IOX Proxy, and WMIC in Multi-Stage Espionage Campaign	https://cybersecuritynews.com/china-aligned-attackers-use-multi-stage-espionage-campaign/
New Fake CAPTCHA Campaign Uses SMS Pumping Fraud to Run Up Victims' Phone Bills	https://cybersecuritynews.com/new-fake-captcha-campaign-uses-sms-pumping/

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

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/