NATIONAL CYBERSECURITY AUTHORITY GR

CVEs Alerts

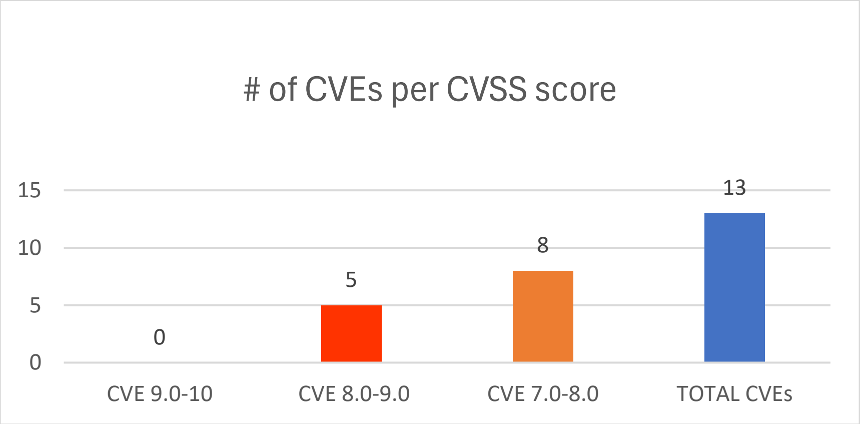
CVEs, CISA/CERT-EU Alerts Advisories & News

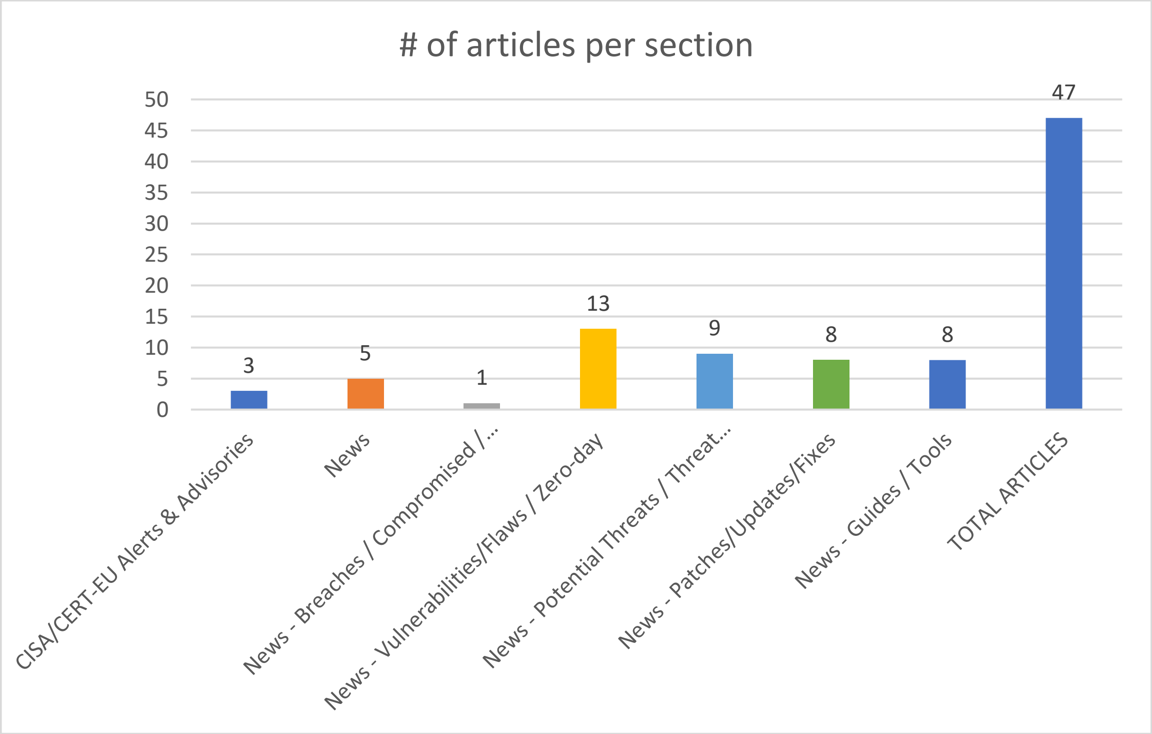
Newsletter on system vulnerabilities and cybersecurity news

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 10/02/2026 - 13/02/2026





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-2026-2315	8.8	WebGPU in Google Chrome		prior to 145.0.7632.45	https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_10.html Chrome https://issues.chromium.org/issues/479242793
https://nvd.nist.gov/vuln/detail/CVE-2026-25759	8.7	Statmatic	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	From 6.0.0 to before 6.2.3	https://github.com/statamic/cms/commit/6ed4f65f3387686d6dbd816e9b4f18a8d9736ff6 GitHub, Inc. https://github.com/statamic/cms/releases/tag/v6.2.3 GitHub, Inc. https://github.com/statamic/cms/security/advisories/GHSA-ff9r-ww9c-43x8
https://nvd.nist.gov/vuln/detail/CVE-2026-25924	8.4	Kanboard	Incorrect Authorization	Prior to 1.2.50	https://github.com/kanboard/kanboard/commit/b9ada89b1a64034612fc4262b88c42458c0d6ee4 GitHub, Inc. https://github.com/kanboard/kanboard/releases/tag/v1.2.50 GitHub, Inc. https://github.com/kanboard/kanboard/security/advisories/GHSA-grch-p7vf-vc4f
https://nvd.nist.gov/vuln/detail/CVE-2026-23857	8.2	Dell Update Package (DUP) Framework	Improper Handling of Insufficient Permissions or Privileges	23.12.00 through 24.12.00	https://www.dell.com/support/kbdoc/en-us/000426781/dsa-2026-081-security-update-for-dell-update-package-dup-framework-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2026-2360	8.0	PostgreSQL Anonymizer	Uncontrolled Search Path Element		https://gitlab.com/dalibo/postgresql_anonymizer/-/blob/latest/NEWS.md PostgreSQL https://gitlab.com/dalibo/postgresql_anonymizer/-/issues/616 PostgreSQL https://www.postgresql.org/docs/current/ddl-schemas.html#DDL-SCHEMAS-PATH

https://nvd.nist.gov/vuln/detail/CVE-2026-25676	7.8	M-Track Duo HD	Uncontrolled Search Path Element	1.0.0	https://jvn.jp/en/jp/JVN88690363/ JPCERT/CC https://www.m-audio.com/audio-midi-interfaces/m-track-duo-hd.html
https://nvd.nist.gov/vuln/detail/CVE-2026-23856	7.8	Dell iDRAC Service Module (iSM) for Windows	Improper Access Control	prior to 6.0.3.1, and Dell iDRAC Service Module (iSM) for Linux, versions prior to 5.4.1.1	https://www.dell.com/support/kbdoc/en-us/000426282/dsa-2026-077-security-update-for-dell-idrac-service-module-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2026-26010	7.6	OpenMetadata	Improper Privilege Management	Prior to 1.11.8	https://github.com/open-metadata/OpenMetadata/releases/tag/1.11.8-release GitHub, Inc. https://github.com/open-metadata/OpenMetadata/security/advisories/GHSA-pqqf-7hxm-rj5r
https://nvd.nist.gov/vuln/detail/CVE-2026-26235	7.5	JUNG Smart Visu Server	Missing Authentication for Critical Function	1.1.1050	https://www.vulncheck.com/advisories/jung-smart-visu-server-jung-smart-visu-server-missing-authentication VulnCheck https://www.zeroscience.mk/en/vulnerabilities/ZSL-2026-5971.php
https://nvd.nist.gov/vuln/detail/CVE-2026-26029	7.5	Salesforce MCP server for Claude	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://github.com/akutishevsky/sf-mcp-server/commit/99fba0171b8c22b5ee3c0405053ccfd2910a066d GitHub, Inc. https://github.com/akutishevsky/sf-mcp-server/security/advisories/GHSA-h4w9-g9c5-vfwq
https://nvd.nist.gov/vuln/detail/CVE-2026-2319	7.5	Race in DevTools in Google Chrome	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	prior to 145.0.7632.45	https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_10.html Chrome https://issues.chromium.org/issues/40071155
https://nvd.nist.gov/vuln/detail/CVE-2026-25999	7.1	Klaw	Improper Authorization	Prior to 2.10.2	https://github.com/Aiven-Open/klaw/commit/617ed96b1db111ed498d89132321bf39f486e3a1 GitHub, Inc. https://github.com/Aiven-Open/klaw/releases/tag/v2.10.2 GitHub, Inc. https://github.com/Aiven-Open/klaw/security/advisories/GHSA-rp26-qv9w-xr5q

https://nvd.nist.gov/vuln/detail/CVE-2026-26158	7.0	BusyBox	External Control of File Name or Path		https://access.redhat.com/security/cve/CVE-2026-26158 Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2439040 Red Hat, Inc. https://git.busybox.net/busybox/commit/archival?id=3fb6b31c716669e12f75a2accd31bb7685b1a1cb

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 Six Known Exploited Vulnerabilities to Catalog	■ CVE-2026-21510 **Microsoft Windows Shell Protection Mechanism Failure Vulnerability** ■ CVE-2026-21513 **Microsoft MSHTML Framework Security Feature Bypass Vulnerability** ■ CVE-2026-21514 **Microsoft Office Word Reliance on Untrusted Inputs in a Security Decision Vulnerability** ■ CVE-2026-21519 **Microsoft Windows Type Confusion Vulnerability** ■ CVE-2026-21525 **Microsoft Windows NULL Pointer Dereference Vulnerability** ■ CVE-2026-21533 **Windows Remote Desktop Services Elevation of Privilege Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/02/10/cisa-adds-six-known-exploited-vulnerabilities-catalog**
Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps		**https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energy-sector-cyber-incident-highlights-ot-and-ics-security-gaps**
Barriers to Secure OT Communication: Why Johnny Can’t Authenticate		**https://www.cisa.gov/resources-tools/resources/barriers-secure-ot-communication-why-johnny-cant-authenticate**

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
Russia Blocked WhatsApp For Over 100 Million Users Nationwide	https://cybersecuritynews.com/russia-blocked-whatsapp/
North Korea's UNC1069 Hammers Crypto Firms With AI	https://www.darkreading.com/threat-intelligence/north-koreas-unc1069-hammers-crypto-firms
FIRST Forecasts Record-Breaking 50,000+ CVEs in 2026	https://www.infosecurity-magazine.com/news/first-forecasts-record-50000-cve/
US Court Hands Crypto Scammer 20 Years in $73m Case	https://www.infosecurity-magazine.com/news/court-hands-crypto-scammer-20-years/
GTIG Analysis Highlights Escalating Espionage and Supply Chain Risks Facing Defense Sector	https://cybersecuritynews.com/gtig-analysis-highlights-escalating-espionage/

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
Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps	https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energy-sector-cyber-incident-highlights-ot-and-ics-security-gaps?&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
Palo Alto Networks Firewall Vulnerability Allows an Attacker to Force Firewalls into a Reboot Loop	https://cybersecuritynews.com/palo-alto-networks-firewall-reboot-loop/
83% of Ivanti EPMM Exploits Linked to Single IP on Bulletproof Hosting Infrastructure	https://thehackernews.com/2026/02/83-of-ivanti-epmm-exploits-linked-to.html
Google-Intel Security Audit Reveals Severe TDX Vulnerability Allowing Full Compromise	https://www.securityweek.com/google-intel-security-audit-reveals-severe-tdx-vulnerability-allowing-full-compromise/
ICS Patch Tuesday: Vulnerabilities Addressed by Siemens, Schneider, Aveva, Phoenix Contact	https://www.securityweek.com/ics-patch-tuesday-vulnerabilities-addressed-by-siemens-schneider-aveva-phoenix-contact/

Windows 11 Notepad flaw let files execute silently via Markdown links	https://www.bleepingcomputer.com/news/microsoft/windows-11-notepad-flaw-let-files-execute-silently-via-markdown-links/
Windows Remote Desktop Services 0-Day Vulnerability Exploited in the Wild to Escalate Privileges	https://cybersecuritynews.com/windows-remote-desktop-services-0-day-vulnerability/
Windows Shell Security Feature 0-Day Vulnerability Let Attackers Bypass Authentication	https://cybersecuritynews.com/windows-shell-security-feature-0-day/
CISA Adds Six Microsoft 0-Day Vulnerabilities to KEV Catalog Following Active Exploitation	https://cybersecuritynews.com/microsoft-0-day-vulnerabilities/
Microsoft Office Word 0-day Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/microsoft-office-word-0-day-vulnerability/
MSHTML Framework 0-Day Vulnerability Let Attackers Security Feature over Network	https://cybersecuritynews.com/mshtml-framework-0-day-vulnerability/
Critical UUID Flaw in Fiber v2 on Go 1.24+ Enables Session Hijacking, CSRF Bypass, and Zero-ID DoS Risk	https://cybersecuritynews.com/uuid-flaw-in-fiber-v2-on-go/
Critical SandboxJS Vulnerability Allows Remote Host Takeover – PoC Released	https://cybersecuritynews.com/sandboxjs-vulnerability-poc-released/
Massive Spike in Attacks Exploiting Ivanti EPMM Systems 0-day Vulnerability	https://cybersecuritynews.com/ivanti-epmm-0-day-flaw-exploited/

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 Patches 59 Vulnerabilities Including Six Actively Exploited Zero-Days	https://thehackernews.com/2026/02/microsoft-patches-59-vulnerabilities.html
Over 60 Software Vendors Issue Security Fixes Across OS, Cloud, and Network Platforms	https://thehackernews.com/2026/02/over-60-software-vendors-issue-security.html
Apple Fixes Exploited Zero-Day Affecting iOS, macOS, and Apple Devices	https://thehackernews.com/2026/02/apple-fixes-exploited-zero-day.html
Ivanti Patches Endpoint Manager Vulnerabilities Disclosed in October 2025	https://www.securityweek.com/ivanti-patches-endpoint-manager-vulnerabilities-disclosed-in-october-2025/
Chipmaker Patch Tuesday: Over 80 Vulnerabilities Addressed by Intel and AMD	https://www.securityweek.com/chipmaker-patch-tuesday-over-80-vulnerabilities-addressed-by-intel-and-amd/
Fortinet Patches High-Severity Vulnerabilities	https://www.securityweek.com/fortinet-patches-high-severity-vulnerabilities/
6 Actively Exploited Zero-Days Patched by Microsoft With February 2026 Updates	https://www.securityweek.com/6-actively-exploited-zero-days-patched-by-microsoft-with-february-2026-updates/
GitLab Patches Multiple Vulnerabilities That Enables DoS and Cross-site Scripting Attacks	https://cybersecuritynews.com/gitlab-patches-dos-xssattacks/

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
Threat Actors Leveraging Employee Monitoring and SimpleHelp Tools to Deploy Ransomware Attacks	https://cybersecuritynews.com/threat-actors-leveraging-employee-monitoring-and-simplehelp-tools/
SSHStalker Botnet Uses IRC C2 to Control Linux Systems via Legacy Kernel Exploits	**https://thehackernews.com/2026/02/sshstalker-botnet-uses-irc-c2-to.html**
Socelars Malware Attacking Windows Systems to Steal Sensitive Business Data	https://cybersecuritynews.com/socelars-malware-attacking-windows-systems/
Sophisticated Cyber Attack Targets Wedding Industry With Teams-Based Malware Delivery	https://cybersecuritynews.com/teams-based-malware-delivery/
Coinbase Cartel Targets High-Value Sectors with Data-Theft-First Extortion Strategy	https://cybersecuritynews.com/coinbase-cartel-targets-high-value-sectors/
Cephalus Ransomware Emerges as Go-Based Double-Extortion Threat Targeting Exposed RDP	https://cybersecuritynews.com/cephalus-ransomware-emerges-as-go-based-double-extortion-threat/
BQTLock & GREENBLOOD Ransomware Attacking Organizations to Encrypt and Exfiltrate Data	https://cybersecuritynews.com/bqtlock-greenblood-ransomware-attacking-organizations/
Threat Actors Weaponize ChatGPT, Grok and Leverages Google Ads to Distribute macOS AMOS Stealer	https://cybersecuritynews.com/threat-actors-weaponize-chatgpt-grok-to-distribute-amos-stealer/
RU-APT-ChainReaver-L Hijacks Trusted Websites and GitHub Repos in Massive Cross-Platform Supply Chain Campaign	https://cybersecuritynews.com/ru-apt-chainreaver-l-hijacks-trusted-websites-and-github-repos/

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/

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/