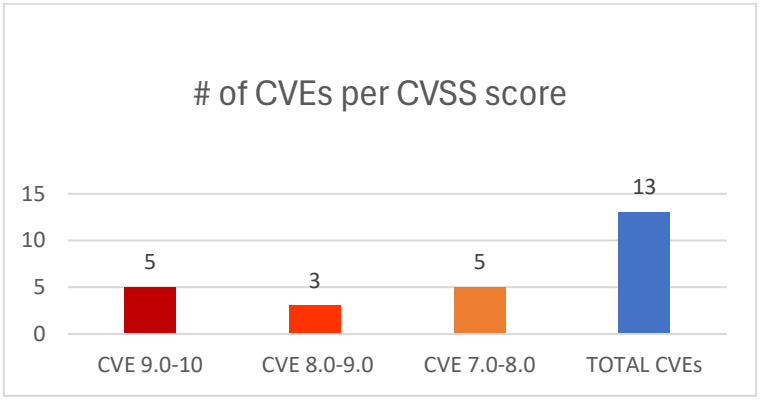
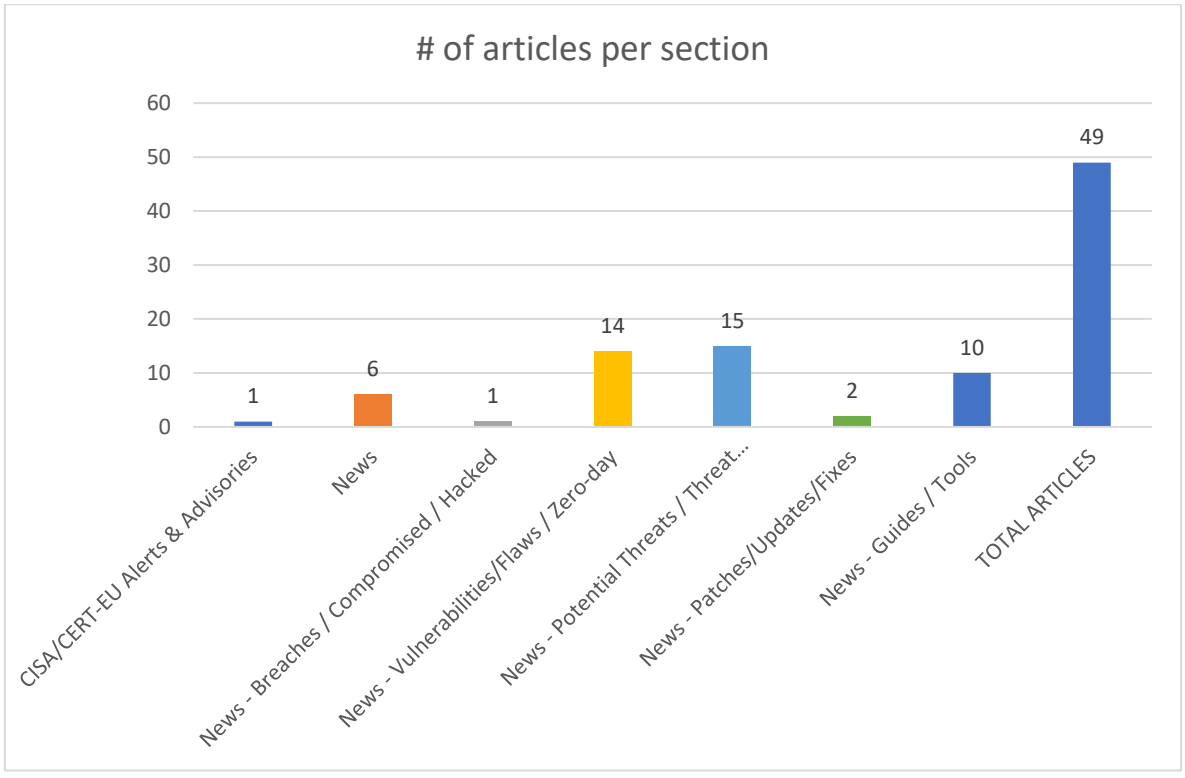
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 07/01/2026 - 09/01/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 5
News 5
Breaches / Compromised / Hacked 6
Vulnerabilities / Flaws / Zero-day 6
Patches / Updates / Fixes 7
Potential threats / Threat intelligence 7
Guides / Tools 8
References 9
Annex – Websites with vendor specific vulnerabilities 10

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-2026-21877	9,9	n8n	Improper Control of Generation of Code ('Code Injection')	0.121.2 and below	https://github.com/n8n-io/n8n/commit/f4b009d00d1f4ba9359b8e8f1c071e3d910a55f6 GitHub, Inc. https://github.com/n8n-io/n8n/security/advisories/GHSA-v364-rw7m-3263
https://nvd.nist.gov/vuln/detail/CVE-2026-22234	9,8	OPEXUS eCasePortal	Authorization Bypass Through User-Controlled Key	before version 9.0.45.0	https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2025/va-26-008-02.json Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government https://www.cve.org/CVERecord?id=CVE-2026-22234
https://nvd.nist.gov/vuln/detail/CVE-2026-21875	9,8	ClipBucket v5	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	5.5.2-#187 and below	https://github.com/MacWarrior/clipbucket-v5/security/advisories/GHSA-crpv-fmc4-j392
https://nvd.nist.gov/vuln/detail/CVE-2026-21876	9,3	The OWASP core rule set (CRS)	Incomplete Filtering of Multiple Instances of Special Elements	Prior to versions 4.22.0 and 3.3.8	https://github.com/coreruleset/coreruleset/commit/80d80473abf71bd49bf6d3c1ab221e3c74e4eb83 GitHub, Inc. https://github.com/coreruleset/coreruleset/commit/9917985de09a6cf38b3261faf9105e909d67a7d6 GitHub, Inc. https://github.com/coreruleset/coreruleset/releases/tag/v3.3.8 GitHub, Inc. https://github.com/coreruleset/coreruleset/releases/tag/v4.22.0 GitHub, Inc. https://github.com/coreruleset/coreruleset/security/advisories/GHSA-36fv-25j3-r2c5
https://nvd.nist.gov/vuln/detail/CVE-2026-21881	9,1	Kanboard	Improper Authentication	1.2.48 and below	https://github.com/kanboard/kanboard/commit/7af6143e2ad25b5c15549cca8af4341c7ac4e2fc GitHub, Inc. https://github.com/kanboard/kanboard/releases/tag/v1.2.49 GitHub, Inc. https://github.com/kanboard/kanboard/security/advisories/GHSA-wwpf-3j4p-739w
https://nvd.nist.gov/vuln/detail/CVE-2026-22257	8,8	Salvo	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to version 0.88.1	https://github.com/salvo-rs/salvo/blob/16efeba312a274739606ce76366d921768628654/crates/serve-static/src/dir.rs#L581 GitHub, Inc.

					https://github.com/salvo-rs/salvo/security/advisories/GHSA-54m3-5fxr-2f3j
https://nvd.nist.gov/vuln/detail/CVE-2026-22255	8,8	iccDEV	Improper Input Validation	prior to 2.3.1.2	https://github.com/InternationalColorConsortium/iccDEV/issues/466 GitHub, Inc. https://github.com/InternationalColorConsortium/iccDEV/pull/469 GitHub, Inc. https://github.com/InternationalColorConsortium/iccDEV/security/advisories/GHSA-qv2w-mq3g-73gv
https://nvd.nist.gov/vuln/detail/CVE-2026-21869	8,8	llama.cpp	Out-of-bounds Write		https://github.com/ggml-org/llama.cpp/security/advisories/GHSA-8947-pfff-2f3c
https://nvd.nist.gov/vuln/detail/CVE-2026-22035	7,7	Greenshot	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1.3.310 and below	https://github.com/greenshot/greenshot/commit/5dedd5c9f0a9896fa0af1d4980d875a48bf432cb GitHub, Inc. https://github.com/greenshot/greenshot/releases/tag/v1.3.311 GitHub, Inc. https://github.com/greenshot/greenshot/security/advisories/GHSA-7hvw-g8q5-gpmj
https://nvd.nist.gov/vuln/detail/CVE-2026-22521	7,5	G5Theme Handmade Framework	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 3.9	https://patchstack.com/database/wordpress/plugin/handmade-framework/vulnerability/wordpress-handmade-framework-plugin-3-9-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-21868	7,5	Flag Forge	Inefficient Regular Expression Complexity	Versions 2.3.2 and below	https://github.com/FlagForgeCTF/flagForge/security/advisories/GHSA-949h-9824-xmcx
https://nvd.nist.gov/vuln/detail/CVE-2026-21873	7,2	NiceGUI	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	From versions 2.22.0 to 3.4.1	https://github.com/zauberzeug/nicegui/releases/tag/v3.5.0 GitHub, Inc. https://github.com/zauberzeug/nicegui/security/advisories/GHSA-mhpg-c27v-6mxr
https://nvd.nist.gov/vuln/detail/CVE-2026-21856	7,2	The Tarkov Data Manager	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://github.com/the-hideout/tarkov-data-manager/commit/9bdb3a75a98a7047b6d70144eb1da1655d6992a8 GitHub, Inc. https://github.com/the-hideout/tarkov-data-manager/security/advisories/GHSA-4gcx-ghwc-rc78

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 Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2009-0556 **Microsoft Office PowerPoint Code Injection Vulnerability** ▪ CVE-2025-37164 **HPE OneView Code Injection Vulnerability**	https://www.cisa.gov/news-events/alerts/2026/01/07/cisa-adds-two-known-exploited-vulnerabilities-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
Hackers Claim to Disconnect Brightspeed Customers After Breach	https://www.infosecurity-magazine.com/news/hackers-disconnect-brightspeed/
China intensifies Cyber-Attacks on Taiwan as Energy Sector Sees Tenfold Spike	https://www.infosecurity-magazine.com/news/china-intensifies-cyberattacks/
Hackers Actively Exploiting AI Deployments – 91,000+ Attack Sessions Observed	https://cybersecuritynews.com/hackers-exploiting-ai-deployments/
Cisco Small Business Switches Face Global DNS Crash Outage	https://cybersecuritynews.com/cisco-small-business-switches-dns-outage/
ChatGPT Health – A Dedicated Space for Health Queries With Strong Privacy and Security	https://cybersecuritynews.com/chatgpt-health/
Trump Signals U.S. Cyber Role in Caracas Blackout During Maduro Capture	https://cybersecuritynews.com/trump-signals-u-s-cyber-role-in-caracas-blackout/

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
Major Data Breach Hits Company Operating 150 Gas Stations in the US	https://hackread.com/data-breach-us-gas-stations-company/?&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
Coolify Discloses 11 Critical Flaws Enabling Full Server Compromise on Self-Hosted Instances	https://thehackernews.com/2026/01/coolify-discloses-11-critical-flaws.html
CISA Flags Microsoft Office and HPE OneView Bugs as Actively Exploited	https://thehackernews.com/2026/01/cisa-flags-microsoft-office-and-hpe.html
Critical n8n Vulnerability (CVSS 10.0) Allows Unauthenticated Attackers to Take Full Control	https://thehackernews.com/2026/01/critical-n8n-vulnerability-cvss-100.html
Veeam Patches Critical RCE Vulnerability with CVSS 9.0 in Backup & Replication	https://thehackernews.com/2026/01/veeam-patches-critical-rce.html
Ongoing Attacks Exploiting Critical RCE Vulnerability in Legacy D-Link DSL Routers	https://thehackernews.com/2026/01/active-exploitation-hits-legacy-d-link.html
Critical HPE OneView Vulnerability Exploited in Attacks	https://www.securityweek.com/critical-hpe-oneview-vulnerability-exploited-in-attacks/
Vulnerability in Totolink Range Extender Allows Device Takeover	https://www.securityweek.com/vulnerability-in-totolink-range-extender-allows-device-takeover/
VMware ESXi zero-days likely exploited a year before disclosure	https://www.bleepingcomputer.com/news/security/vmware-esxi-zero-days-likely-exploited-a-year-before-disclosure/
New Zero-Click Attack Lets ChatGPT User Steal Data	https://www.infosecurity-magazine.com/news/new-zeroclick-attack-chatgpt/
SmarterTools SmarterMail Vulnerability Enables Remote Code Execution Attack – PoC Released	https://cybersecuritynews.com/smartertools-smartermail-vulnerability-poc-released/
Hackers Launched 8.1 Million Attack Sessions to React2Shell Vulnerability	https://cybersecuritynews.com/react2shell-vulnerability-8-1-million-hacks/
Linux Battery Utility Flaw Lets Hackers Bypass Authentication and Tamper System Settings	https://cybersecuritynews.com/linux-battery-utility-flaw/
PoC Exploit Released for Android/Linux Kernel Vulnerability CVE-2025-38352	https://cybersecuritynews.com/chronomaly-exploit/
ToddyCat Malware Compromises Microsoft Exchange Servers using ProxyLogon Vulnerability	https://cybersecuritynews.com/toddycat-malware-compromises-microsoft-exchange-servers/

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
Cisco Patches ISE Security Vulnerability After Public PoC Exploit Release	https://thehackernews.com/2026/01/cisco-patches-ise-security.html
Critical Vulnerability Patched in jsPDF	https://www.securityweek.com/critical-vulnerability-patched-in-jspdf/

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
China-Linked UAT-7290 Targets Telecoms with Linux Malware and ORB Nodes	https://thehackernews.com/2026/01/china-linked-uat-7290-targets-telecoms.html
DDoSia Powers Affiliate-Driven Hacktivist Attacks	**https://www.darkreading.com/cyberattacks-data-breaches/ddosia-powers-volunteer-driven-hacktivist-attacks**
Phishers Exploit Office 365 Users Who Let Their Guard Down	https://www.darkreading.com/cloud-security/phishers-exploit-office-365-users-guard-down
Attackers Exploit Zero-Day in End-of-Life D-Link Routers	https://www.darkreading.com/cyberattacks-data-breaches/attackers-exploit-zero-day-end-of-life-d-link-routers
ChatGPT's Memory Feature Supercharges Prompt Injection	https://www.darkreading.com/endpoint-security/chatgpt-memory-feature-prompt-injection
Critical jsPDF flaw lets hackers steal secrets via generated PDFs	https://www.bleepingcomputer.com/news/security/critical-jspdf-flaw-lets-hackers-steal-secrets-via-generated-pdfs/
Ghost Tap Malware Fuels Surge in Remote NFC Payment Fraud	https://www.infosecurity-magazine.com/news/ghost-tap-malware-remote-nfc-fraud/
Versatile Malware Loader pkr_mtsi Delivers Diverse Payloads	https://www.infosecurity-magazine.com/news/malware-loader-pkrmtsi-payloads/
China-Linked UAT-7290 Targets Telecom Networks in South Asia	https://www.infosecurity-magazine.com/news/china-uat-7290-targets-telecoms/
New Ghost Tapped Attack Uses Your Android Device to Drain Your Bank Account	https://cybersecuritynews.com/new-ghost-tapped-attack-uses-your-android-device/
Hackers Using Malicious Imageless QR Codes to Render Phishing Attack Via HTML Table	https://cybersecuritynews.com/hackers-using-malicious-imageless-qr-codes/
ownCloud Urges Users to Enable Multi-Factor Authentication Following Credential Theft	https://cybersecuritynews.com/owncloud-urges-mfa/
GoBruteforcer Botnet Attacking Linux Servers Worldwide – 50,000 Internet-facing Servers at Risk	https://cybersecuritynews.com/gobruteforcer-botnet/
Researchers Manipulate Stolen Data to Corrupt AI Models and Generate Inaccurate Outputs	https://cybersecuritynews.com/manipulate-stolen-data-corrupt-ai/
LockBit 5.0 Emerges with New Sophisticated Encryption and Anti-Analysis Tactics	https://cybersecuritynews.com/lockbit-5-0-emerges/

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/**
10 Best Vulnerability Management Tools In 2025	https://cybersecuritynews.com/vulnerability-management-tools/
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
Top 15 Best Security Incident Response Tools In 2025	https://cybersecuritynews.com/incident-response-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-tools/
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/
15 Best Remote Monitoring Tools – 2025	https://cybersecuritynews.com/best-remote-monitoring-tools/
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/

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/