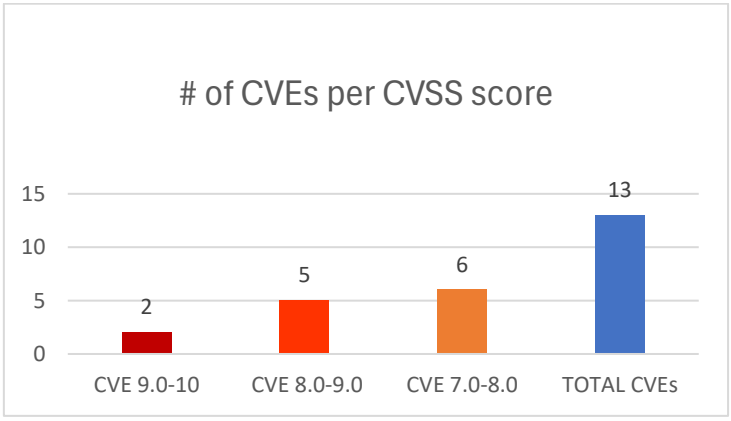
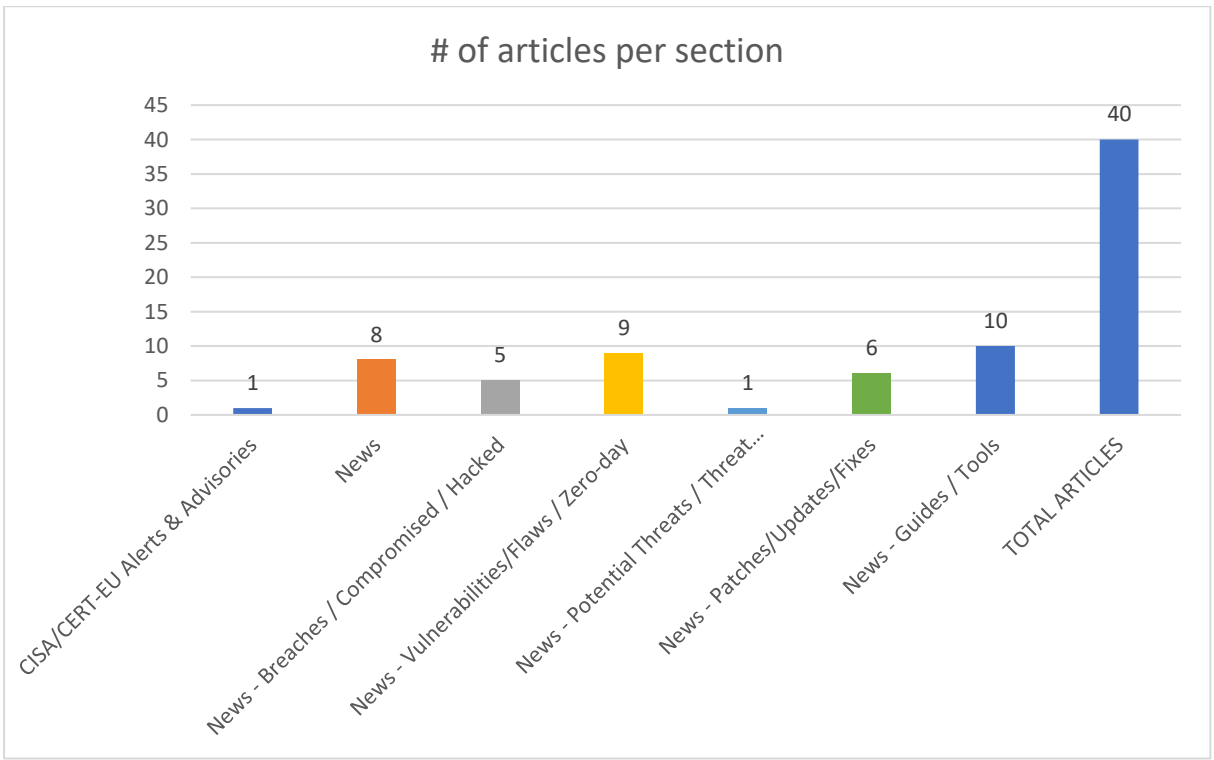
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 06/12/2025 - 09/12/2025





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-2025-12673	9,8	The Flex QR Code Generator plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.2.6	https://github.com/d0n601/CVE-2025-12673 Wordfence https://plugins.trac.wordpress.org/browser/flex-qr-code-generator/trunk/qr-code-generator.php#L457 Wordfence https://ryankozak.com/posts/cve-2025-12673/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/3d71404e-0db8-485b-a626-5e0df2076c05?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13377	9,6	The 10Web Booster – Website speed optimization, Cache & Page Speed optimizer plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 2.32.7	https://plugins.trac.wordpress.org/changeset/3402434/ten-web-speed-optimizer Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/f8bcf51a-36ee-4d4d-b9d6-d9db0dafd791?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-14196	8,8	H3C Magic B1	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 100R004	https://github.com/lin-3-start/lin-cve/blob/main/H3C%20Magic%20B1/H3C%20Magic%20B1.md VulDB https://github.com/lin-3-start/lin-cve/blob/main/H3C%20Magic%20B1/H3C%20Magic%20B1.md#poc VulDB https://vuldb.com/?ctiid.334616 VulDB https://vuldb.com/?id.334616 VulDB https://vuldb.com/?submit.699387
https://nvd.nist.gov/vuln/detail/CVE-2025-14136	8,8	Linksys	Stack-based Buffer Overflow	RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.	https://github.com/wudipjq/my_vuln/blob/main/Linksys2/vuln_65/65.md VulDB https://github.com/wudipjq/my_vuln/blob/main/Linksys2/vuln_65/65.md#poc VulDB https://vuldb.com/?ctiid.334525 VulDB https://vuldb.com/?id.334525 VulDB https://vuldb.com/?submit.697983 VulDB https://www.linksys.com/

				002/1.1.05.003/ 1.2.07.001	
https://nvd.nist.gov/vuln/detail/CVE-2025-13065	**8,8**	The Starter Templates plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 4.4.41	https://plugins.trac.wordpress.org/changeset/3395498/astra-sites/tags/4.4.42/inc/lib/starter-templates-importer/importer/wxr-importer/st-wxr-importer.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/439e4c99-8f34-4e66-9d86-c0cbb8cf6da0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-14126	**8,8**	TOZED ZLT M30S and ZLT M30S PRO	Use of Hard-coded Password	1.47/3.09.06	https://vuldb.com/?ctiid.334521 VulDB https://vuldb.com/?id.334521 VulDB https://vuldb.com/?submit.697498 VulDB https://youtu.be/o8rfjSlpRxY
https://nvd.nist.gov/vuln/detail/CVE-2025-14108	**8,8**	ZSPACE Q2C NAS	Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 1.1.0210050	https://vuldb.com/?ctiid.334490 VulDB https://vuldb.com/?id.334490 VulDB https://vuldb.com/?submit.697144 VulDB https://www.notion.so/2af6cf4e528a80258f60fa529c48d291
https://nvd.nist.gov/vuln/detail/CVE-2025-66623	**7,4**	Strimzi	Incorrect Authorization	From 0.47.0 and prior to 0.49.1	https://github.com/strimzi/strimzi-kafka-operator/commit/c8a14935e99c91eb0dd865431f46515da9f82ccc GitHub, Inc. https://github.com/strimzi/strimzi-kafka-operator/security/advisories/GHSA-xrhh-hx36-485q
https://nvd.nist.gov/vuln/detail/CVE-2025-14258	**7,3**	Student Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/ltranquility/CVE/issues/18 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.334764 VulDB https://vuldb.com/?id.334764 VulDB https://vuldb.com/?submit.702619
https://nvd.nist.gov/vuln/detail/CVE-2025-14188	**7,2**	GREEN DH2100+	Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 5.3.0.251125	https://vuldb.com/?ctiid.334608 VulDB https://vuldb.com/?id.334608 VulDB https://vuldb.com/?submit.698833 VulDB https://www.notion.so/25e2b76e8e0c80578014fff04a950576
https://nvd.nist.gov/vuln/detail/CVE-2025-12499	**7,2**	The Rich Shortcodes for Google Reviews plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 6.8	https://plugins.trac.wordpress.org/changeset/3389203/widget-google-reviews Wordfence https://plugins.trac.wordpress.org/changeset/3411521/widget-google-reviews Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/e2960224-4446-4fc6-8d18-6f9911b4cbad?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-12510	**7,2**	The Widgets for Google Reviews plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 13.2.4	https://plugins.trac.wordpress.org/browser/wp-reviews-plugin-for-google/tags/13.2.1/trustindex-plugin.class.php#L5907 Wordfence https://plugins.trac.wordpress.org/browser/wp-reviews-plugin-for-google/tags/13.2.1/trustindex-plugin.class.php#L5932 Wordfence https://plugins.trac.wordpress.org/changeset/3399469/wp-reviews-plugin-for-google/trunk/trustindex-plugin.class.php?old=3398822&old_path=wp-reviews-plugin-for-google%2Ftrunk%2Ftrustindex-plugin.class.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/7adf3335-ed13-43f4-a5f3-05e89be44d2d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-65363	**7,2**	Ruijie Aps	Improper Neutralization of Special Elements used in a Command ('Command Injection')	AP_RGOS 11.1.x	http://rg-ap720-l.com MITRE http://ruijie.com MITRE https://github.com/tmogg/security-advisories/blob/main/CVE-2025-65363/README.md

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-2022-37055 D-Link Routers Buffer Overflow Vulnerability** ▪ **CVE-2025-66644 Array Networks ArrayOS AG OS Command Injection Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/12/08/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
Researchers Uncover 30+ Flaws in AI Coding Tools Enabling Data Theft and RCE Attacks	https://thehackernews.com/2025/12/researchers-uncover-30-flaws-in-ai.html
US Treasury Tracks $4.5B in Ransom Payments since 2013	https://www.darkreading.com/cyberattacks-data-breaches/us-treasury-45b-ransom-payments-2013
Portugal Revises Cybercrime Law to Protect Security Researchers	https://www.infosecurity-magazine.com/news/portugal-cybercrime-law-security/
Apple, Google and Samsung May Enable Always-On GPS in India	https://cybersecuritynews.com/apple-google-and-samsung-always-on-gps/
NVIDIA and Lakera AI Propose Unified Framework for Agentic System Safety	https://cybersecuritynews.com/nvidia-and-lakera-ai-propose-unified-framework/
Hackers Can Leverage Delivery Receipts on WhatsApp and Signal to Extract User Private Information	https://cybersecuritynews.com/hackers-leverage-delivery-receipts/
The 'Kitten' Project – Hacktivist Groups Carrying Out Attacks Targeting Israel	https://cybersecuritynews.com/the-kitten-project-hacktivist-groups/
FBI Warns of Hackers Altering Photos Found on Social Media to Use as Fake Proof	https://cybersecuritynews.com/fbi-warns-of-hackers-altering-photos/

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
Pharma firm Inotiv discloses data breach after ransomware attack	https://www.bleepingcomputer.com/news/security/pharma-firm-inotiv-discloses-data-breach-after-ransomware-attack/?&web_view=true
Marquis Software Breach Affects Over 780,000 Nationwide	https://www.infosecurity-magazine.com/news/marquis-software-breach/
Crypto User Loses $9,000 in Seconds After Clicking Instagram Ad Promising Easy Profits	https://cybersecuritynews.com/crypto-drainer-scam/
Malicious Go Packages Mimic as Google's UUID Library to Exfiltrate Sensitive Data	https://cybersecuritynews.com/malicious-go-packages-as-googles-uuid-library/
LockBit 5.0 Infrastructure Exposed in New Server, IP, and Domain Leak	https://cybersecuritynews.com/lockbit-5-0-infrastructure-exposed/

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
Critical React2Shell Flaw Added to CISA KEV After Confirmed Active Exploitation	https://thehackernews.com/2025/12/critical-react2shell-flaw-added-to-cisa.html
Sneeit WordPress RCE Exploited in the Wild While ICTBroadcast Bug Fuels Frost Botnet Attacks	https://thehackernews.com/2025/12/sneeit-wordpress-rce-exploited-in-wild.html
Critical Apache Tika Vulnerability Leads to XXE Injection	https://www.securityweek.com/critical-apache-tika-vulnerability-leads-to-xxe-injection/
CISA Warns of D-Link Routers Buffer Overflow Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-d-link-routers-vulnerability/
Critical Cal.com Vulnerability Let Attackers Bypass Authentication Via Fake TOTP Codes	https://cybersecuritynews.com/cal-com-vulnerability/
Critical WatchGuard Firebox Vulnerabilities Let Attackers Bypass Integrity Checks and Inject Malicious Codes	https://cybersecuritynews.com/watchguard-firebox-vulnerabilities/
Critical Vulnerabilities in GitHub Copilot, Gemini CLI, Claude, and Other Tools Impact Millions of Users	https://cybersecuritynews.com/critical-vulnerabilities-in-github-copilot-gemini-cli-claude/
Predator Spyware Compamy Used 15 Zero-Days Since 2021 to Target iOS Users	https://cybersecuritynews.com/predator-spyware-compamy-used-15-zero-days/
Avast Antivirus Sandbox Vulnerabilities Let Attackers Escalate Privileges	https://cybersecuritynews.com/avast-sandbox-escape-vulnerability/

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
SAP Security Patch Day: Fix for Critical Vulnerabilities in SAP Solution Manager, NetWeaver, and Other Products	https://cybersecuritynews.com/sap-security-patch-day-december/

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συν-θήκες. Περι-λαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
MuddyWater Deploys UDPGangster Backdoor in Targeted Turkey-Israel-Azerbaijan Campaign	https://thehackernews.com/2025/12/muddywater-deploys-udpgangster-backdoor.html
ClayRat Android Spyware Expands Capabilities	**https://www.infosecurity-magazine.com/news/clayrat-android-spyware-upgraded/**
New Multi-stage JS#SMUGGLER Malware Attack Delivers 'NetSupport RAT' to Gain Full System Control	https://cybersecuritynews.com/new-multi-stage-jssmuggler-malware-attack/
Malicious Document Reader App in Google Play With 50K Downloads Installs Anatsa Malware	https://cybersecuritynews.com/malicious-document-reader-app-google-play/
OceanLotus Hacker Group Targeting Xinchuang IT Ecosystems to Launch Supply Chain Attacks	https://cybersecuritynews.com/oceanlotus-hacker-group-targeting-xinchuang-it-ecosystems/
New FvncBot Android Banking Attacking Users to Log Keystrokes and Inject Mali-cious Payloads	https://cybersecuritynews.com/fvncbot-android-banking-attacking/

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 επαγ-γελματιών 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/