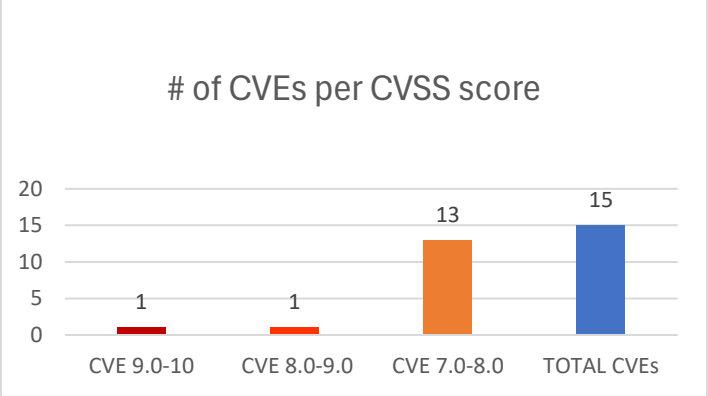
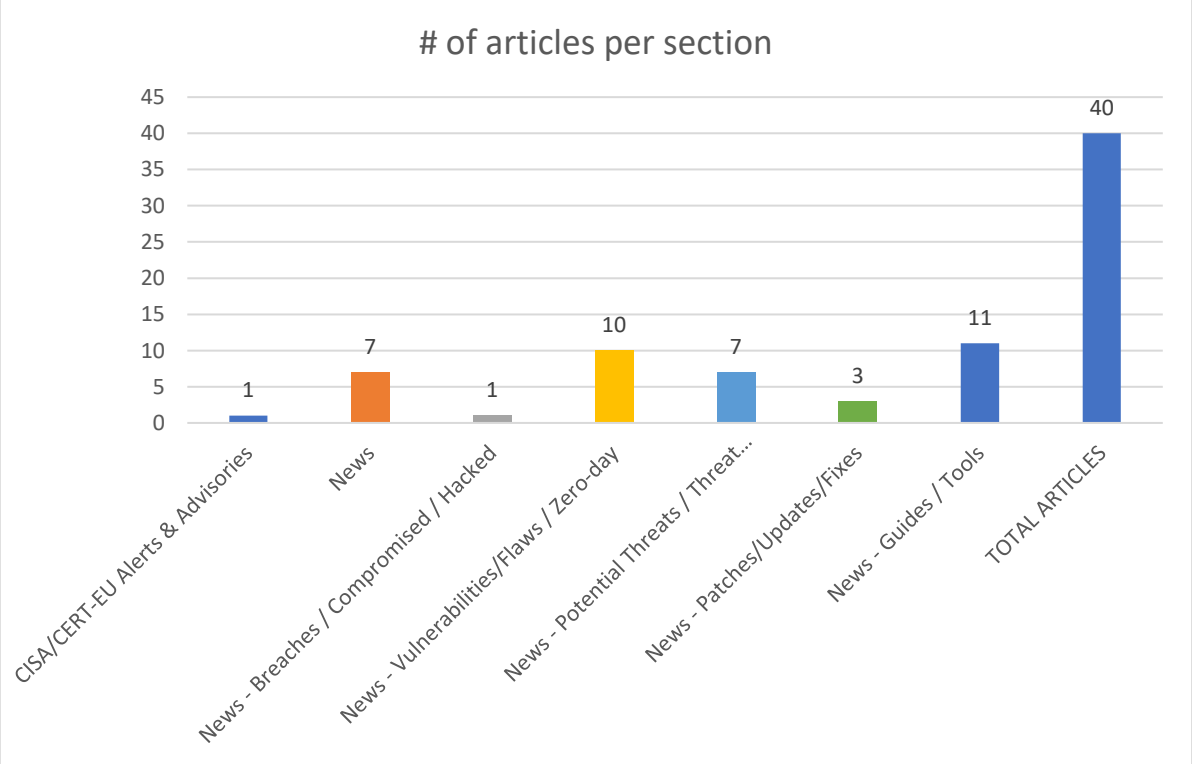
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 08/04/2026 - 10/04/2026





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-2026-5853	9,8	Totolink A7100RU	Improper Neutralization of Special Elements used in a Command ('Command Injection')	7.4cu.2313_b20191024	https://github.com/Li-tengzheng/vuldb_new/blob/main/A7100RU/vul_159/README.md VulDB https://vuldb.com/submit/791274 VulDB https://vuldb.com/vuln/356379 VulDB https://vuldb.com/vuln/356379/cti VulDB https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5173	8,5	GitLab CE/EE	Exposed Dangerous Method or Function	all versions from 16.9.6 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3	https://about.gitlab.com/releases/2026/04/08/patch-release-gitlab-18-10-3-released/ GitLab Inc. https://gitlab.com/gitlab-org/gitlab/-/work_items/588959
https://nvd.nist.gov/vuln/detail/CVE-2026-5301	7,6	CoolerControl/coolercontrol-ui	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	<4.0.0	https://gitlab.com/coolercontrol/coolercontrol/-/blob/2.0.0/coolercontrol-ui/src/views/AppInfoView.vue?ref_type=tags#L224 GitLab Inc. https://gitlab.com/coolercontrol/coolercontrol/-/blob/3.1.1/coolercontrol-ui/src/views/AppInfoView.vue?ref_type=tags#L350 GitLab Inc. https://gitlab.com/coolercontrol/coolercontrol/-/releases/4.0.0
https://nvd.nist.gov/vuln/deta	7,4	In Eclipse Jetty, the class JASPIAuthenticato	Sensitive Information in Resource		https://github.com/jetty/jetty.project/security/advisories/GHSA-r7p8-xq5m-436chttps:// Eclipse Foundation

il/CVE-2026-5795			Not Removed Before Reuse		https://gitlab.eclipse.org/security/cve-assignment/-/issues/92
https://nvd.nist.gov/vuln/detail/CVE-2026-5837	7,3	PHPGurukul News Portal Project	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	4.1	https://github.com/f1rstb100d/CVE/issues/25 VulDB https://phpgurukul.com/ VulDB https://vuldb.com/submit/789775 VulDB https://vuldb.com/vuln/356293 VulDB https://vuldb.com/vuln/356293/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5841	7,3	Tenda	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	i3 1.0.0.6(2204)	https://github.com/MrXiaoFan/Tenda-Vul/tree/main/tenda-i3-V1.0.0.6(2204)-R7WebsSecurityHandler-Authentication%20Bypass%20Issues VulDB https://vuldb.com/submit/789935 VulDB https://vuldb.com/vuln/356297 VulDB https://vuldb.com/vuln/356297/cti VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5842	7,3	decolua 9router	Improper Authorization	up to 0.3.47	https://github.com/decolua/9router/ VulDB https://github.com/decolua/9router/issues/431 VulDB https://github.com/decolua/9router/issues/431#issuecomment-4140163867 VulDB https://github.com/decolua/9router/releases/tag/v0.3.75 VulDB https://github.com/deepcat1337/Free_Api_Exploit/tree/main VulDB https://vuldb.com/submit/790003 VulDB https://vuldb.com/vuln/356298 VulDB https://vuldb.com/vuln/356298/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5802	7,3	idachev mcp-javadc	Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 1.2.4	https://github.com/BruceJqs/public_exp/issues/2 VulDB https://github.com/idachev/mcp-javadc/ VulDB https://github.com/idachev/mcp-javadc/issues/7 VulDB https://vuldb.com/submit/786974 VulDB https://vuldb.com/vuln/356241 VulDB https://vuldb.com/vuln/356241/cti

https://nvd.nist.gov/vuln/detail/CVE-2026-5805	7,3	Easy Blog Site	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	up to 1.0	https://code-projects.org/ VulDB https://github.com/ahmadmarz10-hub/CVEsMarz/blob/main/SQL%20Injection%20in%20Easy%20Blog%20Site%20PHP%20name%20Parameter.md VulDB https://vuldb.com/submit/787031 VulDB https://vuldb.com/vuln/356243 VulDB https://vuldb.com/vuln/356243/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5813	7,3	PHPGurukul Online Course Registration	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	3.1	https://github.com/f1rstb100d/CVE/issues/20 VulDB https://phpgurukul.com/ VulDB https://vuldb.com/submit/787686 VulDB https://vuldb.com/vuln/356261 VulDB https://vuldb.com/vuln/356261/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5824	7,3	Simple Laundry System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/lonelyuan/vunls/issues/1 VulDB https://vuldb.com/submit/788302 VulDB https://vuldb.com/vuln/356271 VulDB https://vuldb.com/vuln/356271/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5827	7,3	Simple IT Discussion Forum	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/lonelyuan/vunls/issues/8 VulDB https://vuldb.com/submit/788336 VulDB https://vuldb.com/vuln/356274 VulDB https://vuldb.com/vuln/356274/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5832	7,3	atototo api-lab-mcp	Server-Side Request Forgery (SSRF)	up to 0.2.1	https://github.com/BruceJqs/public_exp/issues/6 VulDB https://github.com/atototo/api-lab-mcp/ VulDB https://github.com/atototo/api-lab-mcp/issues/4 VulDB https://vuldb.com/submit/789765 VulDB https://vuldb.com/vuln/356288 VulDB https://vuldb.com/vuln/356288/cti

https://nvd.nist.gov/vuln/detail/CVE-2026-5844	7,2	D-Link	Improper Neutralization of Special Elements used in a Command ('Command Injection')	DIR-882 1.01B02	https://nvd.nist.gov/vuln/detail/CVE-2026-5844
https://nvd.nist.gov/vuln/detail/CVE-2026-4808	7,2	The Gerador de Certificados – DevApps plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 1.3.6.	https://plugins.trac.wordpress.org/browser/gerador-de-certificados-devapps/trunk/admin/class-devapps-certificate-generator-admin.php#L346 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/870bf5fe-00c6-48fe-b9e6-e8233c689b71?source=cve

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 One Known Exploited Vulnerability to Catalog	▪ **CVE-2026-1340 Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/04/08/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
Iranian Threat Actors Disrupt US Critical Infrastructure Via Exposed PLCs	https://www.darkreading.com/ics-ot-security/iranian-threat-actors-us-critical-infrastructure-exposed-plcs
Fraud Rockets Higher in Mobile-First Latin America	https://www.darkreading.com/cyberattacks-data-breaches/fraud-mobile-first-latin-america
AI-Led Remediation Crisis Prompts HackerOne to Pause Bug Bounties	https://www.darkreading.com/application-security/ai-led-remediation-crisis-prompts-hackerone-pause-bug-bounties
US Thwarts DNS Hijacking Network Controlled by Russian APT28 Hackers	https://www.infosecurity-magazine.com/news/us-thwarts-dns-hijacking-network/
Claude Discovers Apache ActiveMQ Bug Hidden for 13 Years	https://www.infosecurity-magazine.com/news/claude-apache-activemq-bug-hidden/
Iran-Backed Threat Actors Hit US CNI Providers via Internet-Facing OT Assets	https://www.infosecurity-magazine.com/news/iranbacked-hackers-cni-ot-assets/

Indian Bank Warns Users of Fake LPG Payment and KYC Update Scams to Steal Banking Info	https://cybersecuritynews.com/fake-lpg-payment-and-kyc-update/

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
FBI Disrupts Russian Router Hijacking Operation Compromised Thousands of Users	https://cybersecuritynews.com/fbi-disrupts-russian-router-hijacking/

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
Anthropic's Claude Mythos Finds Thousands of Zero-Day Flaws Across Major Systems	https://thehackernews.com/2026/04/anthropics-claude-mythos-finds.html
RCE Bug Lurked in Apache ActiveMQ Classic for 13 Years	https://www.securityweek.com/rce-bug-lurked-in-apache-activemq-classic-for-13-years/
Hackers Targeting Ninja Forms Vulnerability That Exposes WordPress Sites to Takeover	https://www.securityweek.com/hackers-targeting-critical-ninja-forms-bug-that-exposes-wordpress-sites-to-takeover/
IBM Identity and Verify Access Vulnerabilities Allow Remote Attacker to Access Sensitive Data	https://cybersecuritynews.com/ibm-identity-and-verify-access-vulnerabilities/
Hackers Actively Attacking Adobe Reader Users Using Sophisticated 0-Day Exploit	https://cybersecuritynews.com/adobe-reader-0-day-exploit/
Anthropic Unveils Claude Mythos Preview With Powerful Zero-Day Detection Capabilities	https://cybersecuritynews.com/claude-mythos-zero-day-detection/
Microsoft Confirms Recent Windows 11 Update Breaks Start Menu Search Function	https://cybersecuritynews.com/windows-11-update-breaks-start-menu-function/
Docker Vulnerability Let Attackers Bypass Authorization and Gain Host Access	https://cybersecuritynews.com/docker-vulnerability-bypass-authorization/
Multiple OpenSSL Vulnerabilities Exposes Sensitive Data in RSA KEM Handling	https://cybersecuritynews.com/openssl-vulnerabilities-expose-data/
CUPS Vulnerability Chain Enables Remote Attacker to Execute Malicious Code as Root User	https://cybersecuritynews.com/cups-vulnerability-remote-attack/

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
Data Leakage Vulnerability Patched in OpenSSL	https://www.securityweek.com/data-leakage-vulnerability-patched-in-openssl/
Anthropic Launches Project Glasswing to Use AI to Find and Fix Critical Software Vulnerabilities	https://www.infosecurity-magazine.com/news/anthropic-launch-project-glasswing/
Google Expands Chrome Lazy Loading to Video and Audio in New Browser Update	https://cybersecuritynews.com/google-chrome-lazy-loading/

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
Masjesu Botnet Emerges as DDoS-for-Hire Service Targeting Global IoT Devices	https://thehackernews.com/2026/04/masjesu-botnet-emerges-as-ddos-for-hire.html
APT28 Deploys PRISMEX Malware in Campaign Targeting Ukraine and NATO Allies	https://thehackernews.com/2026/04/apt28-deploys-prismex-malware-in.html
13-year-old bug in ActiveMQ lets hackers remotely execute commands	https://www.bleepingcomputer.com/news/security/13-year-old-bug-in-activemq-lets-hackers-remotely-execute-commands/
Google API Keys Quietly Gain Access to Gemini on Android Devices	https://www.infosecurity-magazine.com/news/google-api-keys-access-gemini/
Microsoft 365 Network-Level Disruption Affecting Exchange Online, Teams, and Core Suite Services	https://cybersecuritynews.com/microsoft-365-network-level-disruption/
Hackers Used EvilTokens, ClickFix Campaign to Attack Claude Code Users with AMOS Stealer	https://cybersecuritynews.com/eviltokens-amos-march-2026-threat-campaigns/
Amazon S3 Files, Turns S3 Buckets as File System to Access Your Data	https://cybersecuritynews.com/amazon-s3-buckets-as-file-system/

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/
PentAGI – Automated AI-Powered Penetration Testing Tool that Integrates 20+ Security Tools	https://cybersecuritynews.com/pentagi-penetration-testing-tool/
The CISO Executive Toolkit (Free Download)	https://thehackernews.uk/wiz-ciso-bundle
Secure Coding Best Practices: Practical Guide + Cheat Sheet for Developers	https://thehackernews.uk/secure-coding-wiz-cheat

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/