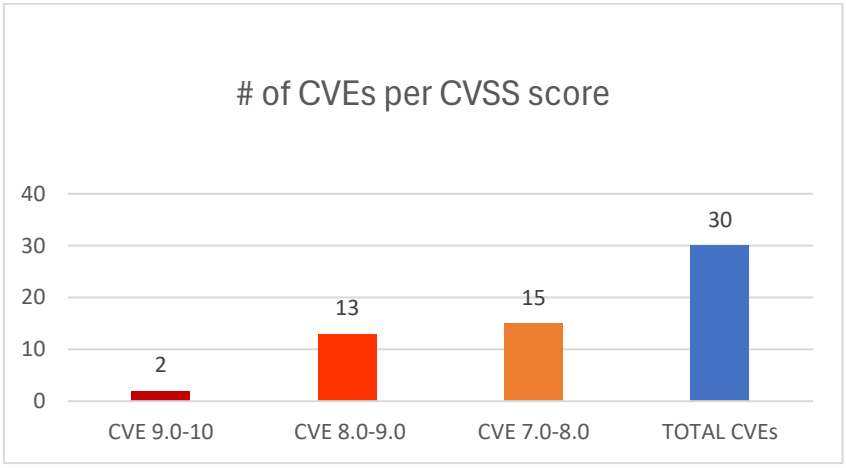
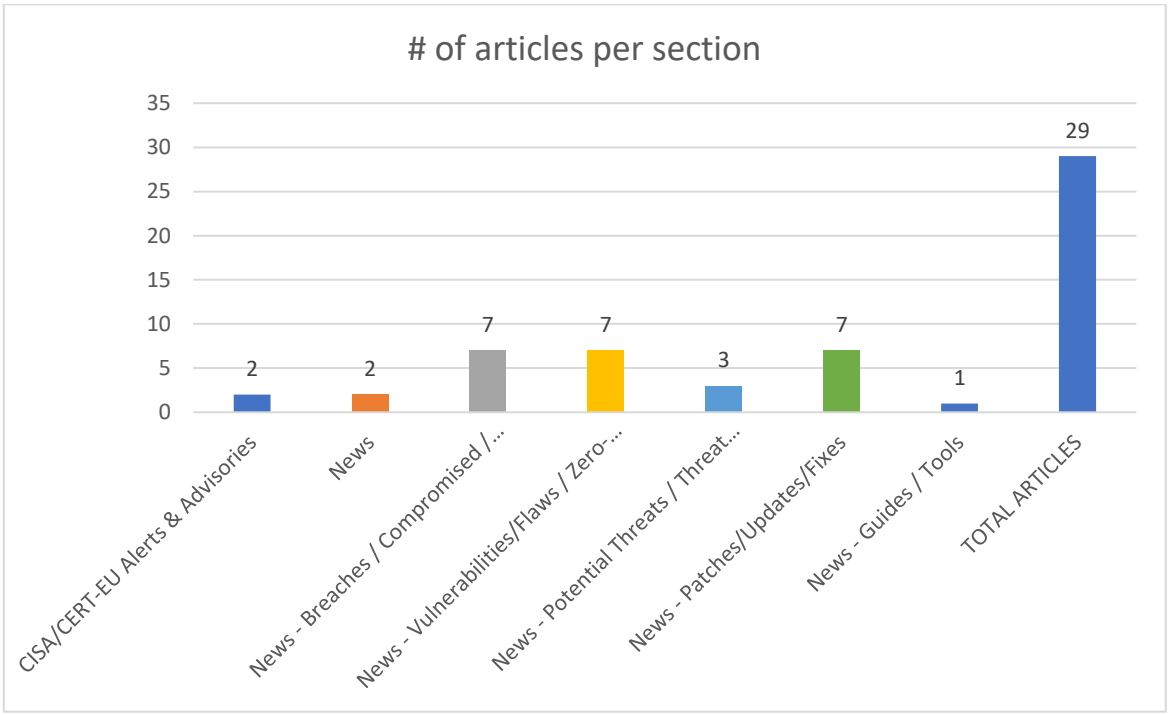
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 10/09/2025 - 12/09/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

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-2025-54123	9.8	Hoverfly	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1.11.3 and prior	https://github.com/SpectoLabs/hoverfly/blob/master/core/hoverfly_service.go#L173 GitHub, Inc. https://github.com/SpectoLabs/hoverfly/blob/master/core/middleware/local_middleware.go#L13 GitHub, Inc. https://github.com/SpectoLabs/hoverfly/blob/master/core/middleware/middleware.go#L93 GitHub, Inc. https://github.com/SpectoLabs/hoverfly/commit/17e60a9bc78826deb4b782dca1c1abd3dbe60d40 GitHub, Inc. https://github.com/SpectoLabs/hoverfly/commit/a9d4da7bd7269651f54542ab790d0c613d568d3e GitHub, Inc. https://github.com/SpectoLabs/hoverfly/security/advisories/GHSA-r4h8-hfp2-ggmf
https://nvd.nist.gov/vuln/detail/CVE-2025-9943	9.1	Shibboleth Service Provider (SP)	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Shibboleth Service Provider through 3.5.0	https://r.sec-consult.com/shibboleth SEC Consult Vulnerability Lab https://shibboleth.net/community/advisories/secadv_20250903.txt SEC Consult Vulnerability Lab https://shibboleth.net/downloads/service-provider/3.5.1/
https://nvd.nist.gov/vuln/detail/CVE-2025-9018	8.8	The Time Tracker plugin for WordPress	Missing Authorization	all versions up to, and including, 3.1.0	https://plugins.trac.wordpress.org/browser/time-tracker/trunk/inc/function-tt-delete-record.php#L22 Wordfence https://plugins.trac.wordpress.org/browser/time-tracker/trunk/inc/function-tt-update-table.php#L25 Wordfence https://plugins.trac.wordpress.org/changeset/3359157/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/2e840f76-1b46-452e-bd63-507cbab779b9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-8557	8.8	Lenovo XClarity Orchestrator (LXCO)	Unprotected Alternate Channel		https://support.lenovo.com/us/en/product_security/LEN-201014

https://nvd.nist.gov/vuln/detail/CVE-2025-8425	8.8	The My WP Translate plugin for WordPress	Missing Authorization	all versions up to, and including, 1.1	https://plugins.trac.wordpress.org/browser/my-wp-translate/tags/1.1/admin/class-my-wp-translate-admin.php#L1116 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/ef46b08f-455a-4c61-81ac-10af19b16980?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7718	8.8	The Resideo Plugin for Resideo - Real Estate WordPress Theme plugin for WordPress	Authorization Bypass Through User-Controlled Key	all versions up to, and including, 2.5.4	https://themeforest.net/item/resideo-real-estate-wordpress-theme/27791406 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/f8375ecf-e64b-4649-9341-fa45bf5556c3?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-56413	8.8	OperateSSH	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1panel 2.0.8	https://github.com/August829/CVEP/issues/5 MITRE https://github.com/August829/Yu/blob/main/20250812_1.md
https://nvd.nist.gov/vuln/detail/CVE-2025-56407	8.8	HuangDou UTCMS	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	V9	https://github.com/August829/CVEP/issues/4 MITRE https://github.com/August829/Yu/blob/main/20250810_1.md
https://nvd.nist.gov/vuln/detail/CVE-2025-55319	8.8	Agentic AI and Visual Studio Code	Ai command injection		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55319
https://nvd.nist.gov/vuln/detail/CVE-2025-10200	8.8	Serviceworker in Google Chrome on Desktop	Use After Free	prior to 140.0.7339.127	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_9.html Chrome https://issues.chromium.org/issues/440454442
https://nvd.nist.gov/vuln/detail/CVE-2025-10201	8.8	Mojo in Google Chrome on Android, Linux, ChromeOS	Improper Access Control	prior to 140.0.7339.127	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_9.html Chrome https://issues.chromium.org/issues/439305148
https://nvd.nist.gov/vuln/detail/CVE-2025-55976	8.4	Intelbras IWR 3000N	Exposure of Sensitive Information to an Unauthorized Actor	1.9.8	https://medium.com/@windsormoreira/intelbras-iwr-3000n-unauthenticated-wi-fi-password-disclosure-cve-2025-55976-7cdac7770413 MITRE https://www.intelbras.com/pt-br/produto/roteador-wireless-n-300mbps-iwr-3000n

https://nvd.nist.gov/vuln/detail/CVE-2025-8417	8.1	The Catalog Importer, Scraper & Crawler plugin for WordPress	Improper Control of Generation of Code ('Code Injection')	all versions up to, and including, 5.1.4	https://plugins.trac.wordpress.org/browser/intelligent-importer/tags/5.1.4/communication.php#L20 Wordfence https://plugins.trac.wordpress.org/browser/intelligent-importer/tags/5.1.4/communication.php#L244 Wordfence https://plugins.trac.wordpress.org/browser/intelligent-importer/tags/5.1.4/communication.php#L272 Wordfence https://plugins.trac.wordpress.org/browser/intelligent-importer/tags/5.1.4/communication.php#L300 Wordfence https://plugins.trac.wordpress.org/browser/intelligent-importer/tags/5.1.4/megaimporter.php#L57 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/3eb3533c-e33c-41db-b9cf-e9d71a0a5588?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9693	8.0	The User Meta – User Profile Builder and User management plugin plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 3.1.2	https://plugins.trac.wordpress.org/browser/user-meta/tags/3.1.2/models/classes/UserInsert.php#L642 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/d482f3a1-4a5a-4382-88b1-fd3b91605694?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-58060	8.0	OpenPrinting CUPS	Improper Authentication	versions 2.4.12 and earlier	https://github.com/OpenPrinting/cups/commit/595d691075b1d396d2edfaa0a8fd0873a0a1f221 GitHub, Inc. https://github.com/OpenPrinting/cups/security/advisories/GHSA-4c68-qgrh-rmmq
https://nvd.nist.gov/vuln/detail/CVE-2025-9201	7.8	Lenovo Browser	Uncontrolled Search Path Element		https://iknow.lenovo.com.cn/detail/431735
https://nvd.nist.gov/vuln/detail/CVE-2025-57392	7.8	BenimPOS Masaustu	Incorrect Permission Assignment for Critical Resource	3.0.x	https://github.com/meisterlos/BenimPOS-POC MITRE https://github.com/meisterlos/CVE-2025-57392
https://nvd.nist.gov/vuln/detail/CVE-2025-50892	7.8	The eudskacs.sys driver	Improper Privilege Management	20250328	http://easeus.com MITRE https://gist.github.com/christopher-ellis-workday/756c998f9f59dd2c437d83e60c7ed220

https://nvd.nist.gov/vuln/detail/CVE-2025-9874	7.5	The Ultimate Classified Listings plugin for WordPress	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	all versions up to, and including, 1.6	https://plugins.trac.wordpress.org/browser/ultimate-classified-listings/trunk/classes/class-shortcodes.php#L49 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/7cf6421c-7b92-4624-9c8a-2a2ab0ca9b28?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9807	7.5	The Events Calendar plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 6.15.1	https://plugins.trac.wordpress.org/browser/the-events-calendar/tags/6.15.0.1/src/Events/Custom_Tables/V1/WP_Query/Custom_Tables_Query.php#L682 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/8ea2ce90-6c8c-4a31-8faa-4ab99879d8b8?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9319	7.5	Lenovo Wallpaper Client	Download of Code Without Integrity Check		https://iknow.lenovo.com.cn/detail/431733
https://nvd.nist.gov/vuln/detail/CVE-2025-9073	7.5	The All in one Minifier plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 3.2	https://plugins.trac.wordpress.org/browser/all-in-one-minifier/trunk/admin/admin-ajax.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/5385ffa7-045b-4ed8-b1d1-eed8924eeb9b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-8696	7.5	the Stork UI	Memory Allocation with Excessive Size Value	Stork versions 1.0.0 through 2.3.0	https://kb.isc.org/docs/cve-2025-8696
https://nvd.nist.gov/vuln/detail/CVE-2025-8422	7.5	The Propovoice: All-in-One Client Management System plugin for WordPress	External Control of File Name or Path	all versions up to, and including, 1.7.6.7	https://plugins.trac.wordpress.org/browser/propovoice/trunk/includes/Api/Type/Email.php#L275 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/3ac72d7a-9540-435f-93cb-fdd4104b18f7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-56406	7.5	mcp-neo4j	Improper Access Control	0.3.0	https://github.com/August829/CVEP/issues/1 MITRE https://github.com/neo4j-contrib/mcp-neo4j/issues/124

https://nvd.nist.gov/vuln/detail/CVE-2025-56404	7.5	MariaDB MCP	Improper Input Validation	0.1.0	https://github.com/August829/CVEP/issues/2 MITRE https://github.com/MariaDB/mcp/issues/17
https://nvd.nist.gov/vuln/detail/CVE-2025-10127	7.3	Daikin Security Gateway	Weak Password Recovery Mechanism for Forgotten Password		https://www.cisa.gov/news-events/ics-advisories/icsa-25-254-10 ICS-CERT https://www.daikin.eu/en_us/customers/support.html
https://nvd.nist.gov/vuln/detail/CVE-2025-8575	7.2	The LWS Cleaner plugin for WordPress	Absolute Path Traversal	all versions up to, and including, 2.4.1.3	https://plugins.trac.wordpress.org/browser/lws-cleaner/trunk/lws-cleaner.php#L1144 Wordfence https://plugins.trac.wordpress.org/changeset/3359598/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/fa37025a-7f20-4cfe-a7d0-38168f49b6d9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-8061	7.0	Lenovo Dispatcher	Exposed IOCTL with Insufficient Access Control	3.0 and Dispatcher 3.1	https://support.lenovo.com/us/en/product_security/LEN-200860
https://nvd.nist.gov/vuln/detail/CVE-2025-10231	7.0	N-central Windows Agent and Probe	Incorrect Default Permissions		https://documentation.n-able.com/N-central/Release_Notes/GA/Content/N-central_2025.3_Release_Notes.htm N-able https://me.n-able.com/s/security-advisory/aArVy0000000jgHKAQ/cve202510231-incorrect-default-permissions-could-lead-to-privilege-escalation

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Eleven Industrial Control Systems Advisories	▪ ICSA-25-254-01 Siemens SIMOTION Tools ▪ ICSA-25-254-02 Siemens SIMATIC Virtualization as a Service (SIVaaS) ▪ ICSA-25-254-03 Siemens SINAMICS Drives ▪ ICSA-25-254-04 Siemens SINEC OS ▪ ICSA-25-254-05 Siemens Apogee PXC and Talon TC Devices ▪ ICSA-25-254-06 Siemens Industrial Edge Management OS (IEM-OS) ▪ ICSA-25-254-07 Siemens User Management Component (UMC) ▪ ICSA-25-254-08 Schneider Electric EcoStruxure ▪ ICSA-25-254-09 Schneider Electric Modicon M340, BMXNOE0100, and BMXNOE0110 ▪ ICSA-25-254-10 Daikin Security Gateway ▪ ICSA-25-035-06 Schneider Electric Modicon M340 and BMXNOE0100/0110, BMXNOR0200H (Update A)	https://www.cisa.gov/news-events/alerts/2025/09/11/cisa-releases-eleven-industrial-control-systems-advisories
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-5086 Dassault Systèmes DELMIA Apriso Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2025/09/11/cisa-adds-one-known-exploited-vulnerability-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
CISA Launches Roadmap for the CVE Program	https://www.infosecurity-magazine.com/news/cisa-launches-roadmap-cve-program/
Ukrainian Ransomware Fugitive Added to Europe's Most Wanted	https://www.infosecurity-magazine.com/news/ukrainian-ransomware-fugitive/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Chinese APT Actor Compromises Military Firm with Novel Fileless Malware Toolset	https://www.infosecurity-magazine.com/news/chinese-apt-military-fileless/
Vienna, VA discloses data breach that leaked SSNs, financial info	https://www.comparitech.com/news/vienna-va-discloses-data-breach-that-leaked-ssns-financial-info/?&web_view=true
Hello Gym Data Leak Exposes 1.6 Million Audio Files of Gym Members	https://hackread.com/hello-gym-data-leak-audio-files-of-gym-members/?&web_view=true
Ransomware attack at blood center: Org tells users their data's been stolen	https://www.malwarebytes.com/blog/news/2025/09/ransomware-attack-at-blood-center-org-tells-users-their-datas-been-stolen?&web_view=true

L7 DDoS Botnet Hijacked 5.76M Devices to Launch Massive Attacks	https://cybersecuritynews.com/l7-ddos-botnet-hijacked-5-76m-devices/
European crypto platform SwissBorg to reimburse users after $41 million theft	https://therecord.media/swissborg-platform-solana-cryptocurrency-stolen?&web_view=true
Cornwell Quality Tools Data Breach – 100,000 Users Data Was Compromised	https://cybersecuritynews.com/cornwell-quality-tools/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Cursor AI Code Editor Flaw Enables Silent Code Execution via Malicious Repositories	https://thehackernews.com/2025/09/cursor-ai-code-editor-flaw-enables.html
Microsoft Patch for Old Flaw Reveals New Kernel Address Leak Vulnerability in Windows 11/Server 2022 24H2	https://cybersecuritynews.com/windows-kernel-address-leak-vulnerability/
Windows Defender Firewall Vulnerabilities Let Attackers Escalate Privileges	https://cybersecuritynews.com/windows-defender-firewall-vulnerabilities/
SonicWall SSL VPN Flaw and Misconfigurations Actively Exploited by Akira Ransomware Hackers	https://thehackernews.com/2025/09/sonicwall-ssl-vpn-flaw-and.html
Cisco Patches High-Severity IOS XR Vulnerabilities	https://www.securityweek.com/cisco-patches-high-severity-ios-xr-vulnerabilities/
Adobe Commerce Flaw CVE-2025-54236 Lets Hackers Take Over Customer Accounts	https://thehackernews.com/2025/09/adobe-commerce-flaw-cve-2025-54236-lets.html
Apple iPhone Air and iPhone 17 Feature A19 Chips With Spyware-Resistant Memory Safety	https://thehackernews.com/2025/09/apple-iphone-air-and-iphone-17-feature.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Fixes 80 Flaws — Including SMB PrivEsc and Azure CVSS 10.0 Bugs	https://thehackernews.com/2025/09/microsoft-fixes-80-flaws-including-smb.html
SAP Patches Critical NetWeaver (CVSS Up to 10.0) and High-Severity S/4HANA Flaws	https://thehackernews.com/2025/09/sap-patches-critical-netweaver-cvss-up.html
Two Zero-Days Among Patch Tuesday CVEs This Month	https://www.infosecurity-magazine.com/news/two-zero-days-patch-tuesday-cves/
VirtualBox 7.2.2 Released With Fix For GUI Crashes On Virtual Machines (guests)	https://cybersecuritynews.com/virtualbox-7-2-2-released/
Critical Chrome Vulnerability Earns Researcher $43,000	https://www.securityweek.com/critical-chrome-vulnerability-earns-researcher-43000/
Fortinet, Ivanti, Nvidia Release Security Updates	https://www.securityweek.com/fortinet-ivanti-nvidia-release-security-updates/
Payment System Vendor Took Year+ to Patch Infinite Card Top-Up Hack: Security Firm	https://www.securityweek.com/payment-system-vendor-took-year-to-patch-infinite-card-top-up-hack-security-firm/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Malicious npm Code Reached 10% of Cloud Environments	https://www.infosecurity-magazine.com/news/malicious-npm-code-10-cloud/
1.5 Billion Packets Per Second DDoS Attack Detected with FastNetMon	https://cybersecuritynews.com/1-5-billion-packets-per-second-ddos-attack-detected/
New Clickfix Attack Promises “Free WiFi” But Delivers Powershell-Based Malware	https://cybersecuritynews.com/clickfix-attack-free-wifi/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/

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/