Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 07/02/2025 - 12/02/2025

Contents

1 Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv 3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	Συσκευές/Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-22467	9.9	Ivanti Connect Secure	Stack-based Buffer Overflow	before version 22.7R2.6	N/A	https://www.ivanti.com/products/connect-secure-vpn https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs
https://nvd.nist.gov/vuln/detail/CVE-2025-24016	9.9	Wazuh	Deserialization of Untrusted Data	Starting in version 4.4.0 and prior to version 4.9.1	N/A	https://wazuh.com/ https://github.com/wazuh/wazuh/security/advisories/GHSA-hcrc-79hj-m3qh
https://nvd.nist.gov/vuln/detail/CVE-2025-0316	9.8	WP Directorybox Manager plugin for WordPress	Authentication Bypass Using an Alternate Path or Channel	up to, and including, 2.5	N/A	https://themeforest.net/item/directory-multipurpose-wordpress-theme/10480929 https://www.wordfence.com/threat-intel/vulnerabilities/id/3ee1f412-7555-4dec-ba59-49412471a42f?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-1044	9.8	Logsign Unified SecOps Platform	Improper Authentication	N/A	N/A	https://www.logsign.com/ https://support.logsign.net/hc/en-us/articles/22076844908946-18-10-2024-Version-6-4-32-Release-Notes https://www.zerodayinitiative.com/advisories/ZDI-25-085/
https://nvd.nist.gov/vuln/detail/CVE-2025-26410	9.8	Wattsense Bridge	Use of Hard-coded Credentials	N/A	firmware BSP >= 6.4.1	https://www.wattsense.com/products/bridge/ https://support.wattsense.com/hc/en-150/articles/13366066529437-Release-Notes https://sec-consult.com/vulnerability-lab/advisory/multiple-vulnerabilities-in-wattsense-bridge/
https://nvd.nist.gov/vuln/detail/CVE-2025-24434	9.1	Adobe Commerce	Improper Authorization	2.4.7-beta1, 2.4.7-p3, 2.4.6-p8, 2.4.5-p10, 2.4.4-p11 and earlier	N/A	https://business.adobe.com/products/magento/magento-commerce.html https://helpx.adobe.com/security/products/magento/apsb25-08.html
https://nvd.nist.gov/vuln/detail/CVE-2024-47908	9.1	Ivanti CSA	OS Command Injection	before version 5.0.5	N/A	https://help.ivanti.com/ld/help/en_US/LDMS/10.0/Windows/csa-h-help.htm https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Services-Application-CSA-CVE-2024-47908-CVE-2024-11771

https://nvd.nist.gov/vuln/detail/CVE-2024-40591	8.8	Fortinet FortiOS	Incorrect Privilege Assignment	7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.9 and before 7.0.15	N/A	https://www.fortinet.com/products/fortigate/fortios https://fortiguard.fortinet.com/psirt/FG-IR-24-302
https://nvd.nist.gov/vuln/detail/CVE-2024-13643	8.8	Zox News - Professional WordPress News & Magazine Theme plugin for WordPress	Missing Authorization	all versions up to and including 3.17.0	N/A	https://themeforest.net/item/zox-news-professional-wordpress-news-magazine-theme/20381541 https://www.wordfence.com/threat-intel/vulnerabilities/id/4adb7436-11e6-4512-b6c9-551402909bf0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-46434	8.8	Tenda W18E	Improper Authentication	V16.01.0.8(1625)	N/A	https://www.tendacn.com/product/overview/w18e.html https://reddassolutions.com/blog/tenda_w18e_security_research
https://nvd.nist.gov/vuln/detail/CVE-2024-27859	8.8	iOS (Apple)	Code Injection	N/A	iOS 17.4 and iPadOS 17.4, tvOS 17.4, watchOS 10.4, visionOS 1.1, macOS Sonoma 14.4	https://www.apple.com/ios/ios-18/ https://support.apple.com/en-us/120881 https://support.apple.com/en-us/120882 https://support.apple.com/en-us/120883 https://support.apple.com/en-us/120893 https://support.apple.com/en-us/120895
https://nvd.nist.gov/vuln/detail/CVE-2024-10383	8.7	GitLab CE/EE	Cross-site Scripting	starting from 15.11 prior to 17.3 and which also temporarily affected versions 17.4, 17.5 and 17.6	N/A	https://about.gitlab.com/install/ce-or-ee/ https://www.tenable.com/cve/CVE-2024-10383
https://nvd.nist.gov/vuln/detail/CVE-2025-24470	8.6	FortiPortal	Improper Resolution of Path Equivalence	7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.11	N/A	https://www.fortinet.com/products/management/fortiportal https://fortiguard.fortinet.com/psirt/FG-IR-25-015
https://nvd.nist.gov/vuln/detail/CVE-2025-25243	8.6	SAP Supplier Relationship Management	Path Traversal	N/A	N/A	https://www.sap.com/products/spend-management/supplier-relationship-management-srm.html https://me.sap.com/notes/3567551 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2025-1143	8.4	Billion Electric	Use of Hard-coded Credentials	N/A	N/A	https://www.billion.com/ https://www.twcert.org.tw/en/cp-139-8414-096ce-2.html https://www.twcert.org.tw/tw/cp-132-8413-ec9a5-1.html
https://nvd.nist.gov/vuln/detail/CVE-2024-7419	8.3	WP ALL Export Pro plugin for WordPress	Code Injection	all versions up to, and including, 1.9.1	N/A	https://www.wpallimport.com/upgrade-to-wp-all-export-pro/ https://www.wordfence.com/threat-intel/vulnerabilities/id/40b57370-4fd7-4316-9e99-a3f1d34616e8?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-24876	8.1	SAP Approuter	URL Redirection to Untrusted Site ('Open Redirect')	version v16.7.1 and before	N/A	https://help.sap.com/docs/BTP/65de2977205c403bbc107264b8eccf4b/01c5f9ba7d6847aaaf069d153b981b51.html https://me.sap.com/notes/3567974 https://url.sap/sapsecuritypatchday

						https://www.npmjs.com/package/@sap/approuter?activeTab=versions
https://nvd.nist.gov/vuln/detail/CVE-2024-57357	8	TPLINK TL-WPA 8630	OS Command Injection	TL-WPA 8630 TL-WPA8630(US)_V2_2.0.4 Build 20230427	N/A	https://www.tp-link.com/se/home-networking/powerline/tl-wpa8630-kit/ https://github.com/c10uds/tplink-wpa8630-rce-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2024-12833	8	Paessler PRTG Network Monitor	Cross-site Scripting	N/A	N/A	https://www.paessler.com/lp/network-monitoring-tool-prtg https://www.zerodayinitiative.com/advisories/ZDI-24-1736/
https://nvd.nist.gov/vuln/detail/CVE-2025-22399	7.9	Dell UCC Edge	Server-Side Request Forgery (SSRF)	2.3.0	N/A	https://www.dell.com/support/product-details/en-us/product/ucc-edge/docs https://www.dell.com/support/kbdoc/en-us/000279299/dsa-2025-043-security-update-for-dell-ucc-edge-security-update-for-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-12755	7.9	Avaya Spaces	Cross-site Scripting	N/A	N/A	https://www.avaya.com/en/ https://support.avaya.com/css/public/documents/101091836
https://nvd.nist.gov/vuln/detail/CVE-2025-22880	7.8	Delta Electronics CNCSoft-G2	Heap-based Buffer Overflow	N/A	N/A	https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=CNCSoft-g2&sort_expr=cdate&sort_dir=DESC https://filecenter.deltaww.com/news/download/doc/Delta-PCSA-2025-00002_CNCSoft-G2%20-%20Heap-based%20Buffer%20Overflow_v1.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-1240	7.8	WinZip	Out-of-bounds Write	N/A	N/A	https://www.winzip.com https://www.zerodayinitiative.com/advisories/ZDI-25-047/
https://nvd.nist.gov/vuln/detail/CVE-2022-26389	7.7	ELI 380 Resting Electrocardiograph	Improper Access Control	Multiple products/versions	N/A	https://www.hillrom.com/en/products/eli-380-electrocardiograph/ https://hillrom.com/en/responsible-disclosures/ https://www.cisa.gov/news-events/ics-medical-advisories/icsma-22-167-01
https://nvd.nist.gov/vuln/detail/CVE-2025-26492	7.7	JetBrains TeamCity	Insufficiently Protected Credentials	before 2024.12.2	N/A	https://www.jetbrains.com/teamcity/ https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2025-24366	7.5	SFTPGo	OS Command Injection	N/A	v2.6.5	https://sftpgo.com/ https://github.com/drakkan/sftpgo/security/advisories/GHSA-vj7w-3m8c-6vpx
https://nvd.nist.gov/vuln/detail/CVE-2025-24811	7.5	SIMATIC S7-1200 (Siemens)	Improper Resource Shutdown or Release	Multiple products/versions	N/A	https://www.siemens.com/gr/el/proionta/automation/systems/industrial/plc/s7-1200.html https://cert-portal.siemens.com/productcert/html/ssa-224824.html

https://nvd.nist.gov/vuln/detail/CVE-2025-0526	7.5	Octopus Deploy	Path Traversal	N/A	N/A	https://octopus.com/ https://advisories.octopus.com/post/2024/sa2025-03/
https://nvd.nist.gov/vuln/detail/CVE-2024-54089	7.5	APOGEE PXC Series (BACnet), APOGEE PXC Series (P2 Ethernet) , TALON TC Series (BACnet) (Siemens)	Inadequate Encryption Strength	All versions	N/A	https://sid.siemens.com/v/u/A6V10304985 https://cert-portal.siemens.com/productcert/html/ssa-615116.html
https://nvd.nist.gov/vuln/detail/CVE-2025-23363	7.4	Teamcenter (Siemens)	URL Redirection to Untrusted Site ('Open Redirect')	All versions < V14.3.0.0	N/A	https://plm.sw.siemens.com/en-US/teamcenter https://cert-portal.siemens.com/productcert/html/ssa-656895.html
https://nvd.nist.gov/vuln/detail/CVE-2025-1104	7.3	D-Link DHP-W310AV	Improper Authentication	1.04	N/A	https://www.dlink.com/gr/el/products/dhp-w310av-powerline-av-500-wireless-n-extender https://github.com/kn1g78/cve/blob/main/dlink.md
https://nvd.nist.gov/vuln/detail/CVE-2024-50567	7.2	Fortinet FortiWeb	OS Command Injection	7.4.0 through 7.6.0	N/A	https://www.fortinet.com/products/web-application-firewall/fortiweb https://fortiguard.fortinet.com/psirt/FG-IR-24-438
https://nvd.nist.gov/vuln/detail/CVE-2024-40584	7.2	Fortinet FortiAnalyzer	OS Command Injection	Multiple products/versions	N/A	https://www.fortinet.com/products/management/fortianalyzer https://fortiguard.fortinet.com/psirt/FG-IR-24-220
https://nvd.nist.gov/vuln/detail/CVE-2024-27781	7.1	Fortinet FortiSandbox	Cross-site Scripting	4.4.0 through 4.4.4 and 4.2.0 through 4.2.6 and 4.0.0 through 4.0.4 and 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.0 through 3.0.7	N/A	https://www.fortinet.com/products/fortisandbox https://fortiguard.fortinet.com/psirt/FG-IR-24-063
https://nvd.nist.gov/vuln/detail/CVE-2024-13813	7.1	Ivanti Secure Access Client	Incorrect Permission Assignment for Critical Resource	before version 22.8R1	N/A	https://www.ivanti.com/products/secure-unified-client https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Known Exploited Vulnerability to Catalog	CVE-2025-0994 Trimble Cityworks Deserialization Vulnerability CVE-2024-40891 Zyxel DSL CPE OS Command Injection Vulnerability CVE-2024-40890 Zyxel DSL CPE OS Command Injection Vulnerability CVE-2025-21418 Microsoft Windows Ancillary Function Driver for WinSock Heap-Based Buffer Overflow Vulnerability CVE-2025-21391 Microsoft Windows Storage Link Following Vulnerability	https://www.cisa.gov/news-events/alerts/2025/02/07/cisa-adds-one-known-exploited-vulnerability-catalog https://www.cisa.gov/news-events/alerts/2025/02/11/cisa-adds-four-known-exploited-vulnerabilities-catalog
CISA Releases Two Industrial Control Systems Advisories	ICSA-24-319-17 2N Access Commander (Update A) ICSA-25-037-04 Trimble Cityworks (Update A)	https://www.cisa.gov/news-events/alerts/2025/02/11/cisa-releases-two-industrial-control-systems-advisories
Vulnerability Summary for the Week of February 3, 2025	Common Vulnerabilities and Exposures (CVE)	https://www.cisa.gov/news-events/bulletins/sb25-041

3 News

Σύντομη περιγραφή / Τίτλος	URL
UK Gov demands backdoor to access Apple iCloud backups worldwide	https://securityaffairs.com/174032/laws-and-regulations/uk-gov-demands-backdoor-apple-icloud-backups.html
SECURITY AFFAIRS MALWARE NEWSLETTER – ROUND 32	https://securityaffairs.com/174025/malware/security-affairs-malware-newsletter-round-32.html
Week in review: Exploited 7-Zip 0-day flaw, crypto-stealing malware found on App Store, Google Play	https://www.helpnetsecurity.com/2025/02/09/week-in-review-exploited-7-zip-0-day-flaw-crypto-stealing-malware-found-on-app-store-google-play/
Russia's intelligence recruits Ukrainians for terror attacks via messaging apps	https://securityaffairs.com/173980/breaking-news/russias-intelligence-recruits-ukrainians-for-terror-attacks.html
SolarWinds to Go Private for $4.4B	https://www.darkreading.com/cybersecurity-operations/solarwinds-private-billions
Cybersecurity Weekly Brief: Latest on Attacks, Vulnerabilities, & Data Breaches	https://cybersecuritynews.com/cybersecurity-weekly-brief-feb-3-to-9/
World's Longest and Strongest WiFi Passwords From 31 Million Passwords List	https://cybersecuritynews.com/worlds-longest-and-strongest-wifi-passwords/
THN Weekly Recap: Top Cybersecurity Threats, Tools and Tips [10 February]	https://thehackernews.com/2025/02/thn-weekly-recap-top-cybersecurity_10.html

Paragon Spyware Used in WhatsApp Hacking Scandal	https://dailysecurityreview.com/security-spotlight/paragon-spyware-used-in-whatsapp-hacking-scandal/
Cyberattacks targeting medical organizations up 32% in 2024	https://www.scworld.com/news/cyberattacks-targeting-medical-organizations-up-32-in-2024

3.1 Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Teen Hacker “Natohub” Caught for NATO, UN, and US Army Breaches	https://hackread.com/teen-hacker-natohub-caught-nato-un-us-army-breach/
HPE notifies employees of data breach after Russian Office 365 hack	https://www.bleepingcomputer.com/news/security/hpe-notifies-employees-of-data-breach-after-russian-office-365-hack/
US health system notifies 882,000 patients of August 2023 breach	https://www.bleepingcomputer.com/news/security/us-health-system-notifies-882-000-patients-of-august-2023-breach/
Cisco Hacked – Ransomware Group Allegedly Breach Internal Network & Gained AD Access	https://cybersecuritynews.com/cisco-hacked/
Hackers Allegedly Claiming Breach OmniGPT, 30,000+ User Accounts Exposed	https://cybersecuritynews.com/hackers-allegedly-claiming-breach-omnigpt/

3.2 Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
XE Hacker Group Exploits VeraCore Zero-Day to Deploy Persistent Web Shells	https://thehackernews.com/2025/02/xe-hacker-group-exploits-veracore-zero.html
Behind the Message: Two Critical XSS Vulnerabilities in Zoho’s Web Applications	https://infosecwriteups.com/behind-the-message-two-critical-xss-vulnerabilities-in-zohos-web-applications-86aa42887129
Seven Years Old Linux Kernel Vulnerability Let Attackers Execute Remote Code	https://cybersecuritynews.com/seven-years-old-linux-kernel-flaw/
PoC Exploit Released for AnyDesk Vulnerability Exploited to Gain Admin Access Via Wallpapers	https://cybersecuritynews.com/poc-exploit-released-for-anydesk-vulnerability-exploited/
Over 12,000 KerioControl firewalls exposed to exploited RCE flaw	https://www.bleepingcomputer.com/news/security/over-12-000-keriocontrol-firewalls-exposed-to-exploited-rce-flaw/
Attackers exploit a new zero-day to hijack Fortinet firewalls	https://securityaffairs.com/174117/hacking/fortinet-fortios-zero-day-exploited.html
Mirai Botnet Exploting Router Vulnerabilities to Gain Complete Device Control	https://cybersecuritynews.com/mirai-botnet-exploiting-router-vulnerabilities/
Remote Desktop Manager Vulnerabilities Let Attackers Intercept Encrypted Communications	https://cybersecuritynews.com/rdm-vulnerabilities-intercept-encrypted-communications/

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Zimbra Releases Security Updates for SQL Injection, Stored XSS, and SSRF Vulnerabilities	https://thehackernews.com/2025/02/zimbra-releases-security-updates-for.html
Fixing stdlib 1.18.2 Vulnerabilities in Docker Images: A PostgreSQL Implementation Guide	https://infosecwriteups.com/fixing-stdlib-1-18-2-vulnerabilities-in-docker-images-a-postgresql-implementation-guide-358183e0dd76
Microsoft shares workaround for Windows security update issues	https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-workaround-for-windows-security-update-issues/
Microsoft's Patch Tuesday Fixes 63 Flaws, Including Two Under Active Exploitation	https://thehackernews.com/2025/02/microsofts-patch-tuesday-fixes-63-flaws.html
Ivanti Patches Critical Flaws in Connect Secure and Policy Secure – Update Now	https://thehackernews.com/2025/02/ivanti-patches-critical-flaws-in.html
Progress Software fixed multiple high-severity LoadMaster flaws	https://securityaffairs.com/174103/security/progress-software-loadmaster-software-flaws.html
SonicWall firewall exploit lets hackers hijack VPN sessions, patch now	https://www.bleepingcomputer.com/news/security/sonicwall-firewall-exploit-lets-hackers-hijack-vpn-sessions-patch-now/
Apple Releases Urgent Patch for USB Vulnerability	https://www.darkreading.com/endpoint-security/apple-releases-urgent-patch-usb-vulnerability
OpenSSL patched high-severity flaw CVE-2024-12797	https://securityaffairs.com/174111/security/openssl-patched-the-vulnerability-cve-2024-12797.html
SAP Security Update – 19 Vulnerabilities Across Multiple Products Patched	https://cybersecuritynews.com/19-vulnerabilities-across-multiple-products-patched/

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Scammers Use Fake Facebook Copyright Notices to Hijack Accounts	https://hackread.com/scammers-use-fake-facebook-copyright-notices-to-hijack-accounts/
Europol Warns Financial Sector of “Imminent” Quantum Threat	https://www.infosecurity-magazine.com/news/europol-warns-financial-sector/
Massive brute force attack uses 2.8 million IPs to target VPN devices	https://www.bleepingcomputer.com/news/security/massive-brute-force-attack-uses-28-million-ips-to-target-vpn-devices/
Widespread Android malware campaign hits India	https://www.scworld.com/brief/widespread-android-malware-campaign-hits-india
Quishing via QR Codes Emerging As a Top Attack Vector Used by Hackers	https://cybersecuritynews.com/quishing-via-qr-codes-emerging-as-a-top-attack-vector/
SAML Bypass Authentication on GitHub Enterprise Servers To Login as Other User Account	https://cybersecuritynews.com/saml-bypass-authentication-on-github-enterprise-servers/

Apple Confirms ‘Extremely Sophisticated’ Exploit Threatening iOS Security	https://hackread.com/apple-extremely-sophisticated-exploit-ios-security/
North Korean Hackers Exploit PowerShell Trick to Hijack Devices in New Cyberattack	https://thehackernews.com/2025/02/north-korean-hackers-exploit-powershell.html

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Tor Browser 14.0.6 Released, What’s New!	https://cybersecuritynews.com/tor-browser-14-0-6-released/
10 Best UTM (Unified Threat Management) Firewalls – 2025	https://cybersecuritynews.com/best-utm-software/
SysReptor: Open-source penetration testing reporting platform	https://www.helpnetsecurity.com/2025/02/12/sysreptor-open-source-penetration-testing-reporting-platform/

4 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.

[3]. Τα CVEs που αφορούν Wordpress plugins θα εμφανίζονται σε ξεχωριστή ενότητα (1.1) σε περιόδους που η εμφάνισή τους είναι ιδιαίτερα αυξημένη.

5 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/