Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 14/012024 - 17/01/2025

Contents

1 Common Vulnerabilities and Exposures (CVE)

CVEs						
URL ευπάθειας (NIST NVD)	**CVSSv3**	**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-2024-39761	**10**	Wavlink AC3000	Command Injection	M33A8.V5030.210505	N/A	https://www.wavlink.com/en_us/product/WL-WN533A8.html https://talosintelligence.com/vulnerability_reports/TALOS-2024-2018
https://nvd.nist.gov/vuln/detail/CVE-2025-0471	**9.9**	PMB platform	Unrestricted Upload of File with Dangerous Type	4.0.10 and above	N/A	https://www.sigb.net https://www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-pmb-platform
https://nvd.nist.gov/vuln/detail/CVE-2024-48856	**9.8**	QNX Software Development Platform	Out-of-bounds Write	8.0, 7.1 and 7.0	N/A	https://blackberry.qnx.com/en/products/foundation-software/qnx-software-development-platform https://support.blackberry.com/pkb/s/article/140334
https://nvd.nist.gov/vuln/detail/CVE-2024-13161	**9.8**	Ivanti EPM	Absolute Path Traversal	before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update	N/A	https://www.manageengine.com/products/desktop-central/endpoint-management.html https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6
https://nvd.nist.gov/vuln/detail/CVE-2024-55591	**9.8**	FortiOS and FortiProxy	Authentication Bypass	FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12	N/A	https://www.fortinet.com/products/fortigate/fortios https://fortiguard.fortinet.com/psirt/FG-IR-24-535
https://nvd.nist.gov/vuln/detail/CVE-2024-12919	**9.8**	Paid Membership Subscriptions – Effortless Memberships, Recurring Payments & Content Restriction plugin for WordPress	Improper Authentication	all versions up to, and including, 2.13.7	N/A	https://wordpress.org/plugins/paid-member-subscriptions/ https://www.wordfence.com/threat-intel/vulnerabilities/id/d3a4fa4d-a7d2-4890-b0f5-5fe69bc5e7ac?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-57684	**9.8**	D-Link 816	Incorrect Default Permissions	A2_FWv1.10CNB05_R1B011D88210	N/A	https://www.dlink.com/gr/el/products/dir-816l-wireless-ac750-cloud-router https://www.dlink.com/en/security-bulletin/

https://nvd.nist.gov/vuln/detail/CVE-2025-22912	9.8	Edimax RE11S	Code Injection	v1.11	N/A	https://www.edimax.com/edimax/merchandise/merchandise_detail/data/edimax/global/whole_home_wifi_system_ac1200_dual-band/re11s/ https://github.com/xyqer1/RE11S_1.11-formAccept-CommandInjection https://www.edimax.com/edimax/global/
https://nvd.nist.gov/vuln/detail/CVE-2025-0456	9.8	airPASS from NetVision	Missing Authentication for Critical Function	N/A	N/A	https://www.net-vision.co.jp/sv-english/ https://www.twcert.org.tw/en/cp-139-8360-e97b8-2.html
https://nvd.nist.gov/vuln/detail/CVE-2024-57022	9.8	TOTOLINK X5000R	OS Command Injection	V9.1.0cu.2350_B20230313	N/A	https://www.totolink.net/home/menu/newstpl/menu_newstpl/products/id/218.html https://github.com/tiger5671/Vulnerabilities/blob/main/TOTOLINK%20X5000R/setWiFiScheduleCfg/setWiFiScheduleCfg.md https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-22968	9.8	D-Link DWR-M972V	Code Injection	1.05SSG	N/A	https://shop.dlink.com.sg/products/4g-ac1200-lte-gigabit-dual-band-mobile-wireless-wifi-hotspot-router-with-nano-sim-slot-dwr-m972v https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2024-12084	9.8	rsync	Heap-based Buffer Overflow	N/A	N/A	https://linux.die.net/man/1/rsync http://www.openwall.com/lists/oss-security/2025/01/14/6 https://access.redhat.com/security/cve/CVE-2024-12084
https://nvd.nist.gov/vuln/detail/CVE-2024-9636	9.8	Post Grid and Gutenberg Blocks plugin for WordPress	Improper Privilege Management	2.2.85 to 2.3.3	N/A	https://wordpress.org/plugins/ultimate-post/ https://www.wordfence.com/threat-intel/vulnerabilities/id/1bbe01b8-24ed-4e1e-bafc-0f4dea96c1f3?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-57483	9.8	Tenda i24	Classic Buffer Overflow	V2.0.0.5	N/A	https://www.tendacn.com/product/i24.html http://tenda.com https://gist.github.com/XiaoCurry/7dd5c6ab5af9df49883535b997cef7a4
https://nvd.nist.gov/vuln/detail/CVE-2024-44136	9.1	iOS 17.5 and iPadOS 17.5	disable Stolen Device Protection	iOS 17.5 and iPadOS 17.5	N/A	https://el.wikipedia.org/wiki/IOS https://support.apple.com/en-us/120905
https://nvd.nist.gov/vuln/detail/CVE-2024-11497	8.8	Phoenix Contact (CHARX SEC products)	Incorrect Permission Assignment for Critical Resource	CHARX SEC-3000 < 1.7.0 CHARX SEC-3050 < 1.7.0 CHARX SEC-3100 < 1.7.0 CHARX SEC-3150 < 1.7.0	N/A	https://www.phoenixcontact.com/en-pc/products/ac-charging-controller-charx-sec-3000-1139022 https://cert.vde.com/en/advisories/VDE-2024-070
https://nvd.nist.gov/vuln/detail/CVE-2024-57726	8.8	SimpleHelp remote support software	escalate privileges	v5.5.7 and before	N/A	https://simple-help.com/ https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier
https://nvd.nist.gov/vuln/detail/CVE-2025-0447	8.8	Google Chrome	Cross-site Scripting	prior to 132.0.6834.83	N/A	https://www.google.com/chrome/ https://issues.chromium.org/issues/375550814

https://nvd.nist.gov/vuln/detail/CVE-2024-55954	8.7	OpenObserve is a cloud-native observability platform	Improper Privilege Management	N/A	N/A	https://openobserve.ai/ https://github.com/openobserve/openobserve/security/advisories/GHSA-m8gj-6r85-3r6m
https://nvd.nist.gov/vuln/detail/CVE-2024-47140	8.7	Observium CE	Cross-site Scripting	24.4.13528	N/A	https://www.observium.org/ https://www.talosintelligence.com/vulnerability_reports/TALOS-2024-2090
https://nvd.nist.gov/vuln/detail/CVE-2024-12365	8.5	W3 Total Cache plugin for WordPress	Missing Authorization	all versions up to, and including, 2.8.1	N/A	https://wordpress.org/plugins/w3-total-cache/ https://www.wordfence.com/threat-intel/vulnerabilities/id/196e629f-7c77-4bcb-8224-305a0108b630?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-40771	8.4	macOS	Incorrect Authorization	Sonoma 14.5, iOS 16.7.8 and iPadOS 16.7.8, iOS 17.5 and iPadOS 17.5, macOS Monterey 12.7.5, watchOS 10.5, tvOS 17.5, macOS Ventura 13.6.7, visionOS 1.2	N/A	https://el.wikipedia.org/wiki/MacOS https://support.apple.com/en-us/120898 https://support.apple.com/en-us/120899 https://support.apple.com/en-us/120900 https://support.apple.com/en-us/120901 https://support.apple.com/en-us/120902 https://support.apple.com/en-us/120903 https://support.apple.com/en-us/120905 https://support.apple.com/en-us/120906
https://nvd.nist.gov/vuln/detail/CVE-2024-11848	8.1	NitroPack plugin for WordPress	Missing Authorization	all versions up to, and including, 1.17.0	N/A	https://wordpress.org/plugins/nitropack/ https://www.wordfence.com/threat-intel/vulnerabilities/id/1e1b06d0-f348-4a8b-8730-a87d8e2ba2a1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-21325	7.8	Windows Secure Kernel Mode	Elevation of Privilege	N/A	N/A	https://learn.microsoft.com/en-us/windows-server/security/kernel-mode-hardware-stack-protection https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21325
https://nvd.nist.gov/vuln/detail/CVE-2024-42444	7.5	APTIOV	Race Condition	N/A	N/A	https://www.ami.com/aptio/ https://go.ami.com/hubfs/Security%20Advisories/2025/AMI-SA-2025001.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-13333	7.5	Advanced File Manager plugin for WordPress	Unrestricted Upload of File with Dangerous Type	5.2.12 to 5.2.13	N/A	https://wordpress.org/plugins/file-manager-advanced/ https://www.wordfence.com/threat-intel/vulnerabilities/id/1c8bcbf8-1848-4f7a-89d8-5894de0bb18b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-0492	7.5	D-Link DIR-823X	Improper Resource Shutdown or Release	240126/240802	N/A	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10404 https://tasty-foxtrot-3a8.notion.site/D-link-DIR-823X-FUN_00412244-NULL-Pointer-Dereference-1730448e619580fcb7f9d871c6e7190a
https://nvd.nist.gov/vuln/detail/CVE-2024-11322	7.5	CyberPower PowerPanel Business (PPB)	Improper Authentication	4.11.0	N/A	https://www.cyberpower.com/eu/en/product/series/powerpanel_business https://www.tenable.com/security/research/tra-2025-01
https://nvd.nist.gov/vuln/detail/CVE-2024-50338	7.4	Git Credential Manager	Exposure of Sensitive Information	N/A	N/A	https://github.com/git-ecosystem/git-credential-manager https://github.com/git-ecosystem/git-credential-manager/releases/tag/v2.6.1
https://nvd.nist.gov/vuln/detail/CVE-2025-23051	7.2	AOS-8 and AOS-10 Operating Systems	authenticated parameter injection	N/A	N/A	https://www.arubanetworks.com/techdocs/central/latest/content/aos10x/aos10x-overview/architecture-overview-aos10.htm https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04723en_us&docLocale=en_US

https://nvd.nist.gov/vuln/detail/CVE-2024-41746	7.2	IBM CICS TX	Cross-site Scripting	Advanced 10.1, 11.1, and Standard 11.1	N/A	https://www.ibm.com/docs/en/cics-tx/11.1?topic=tx-introduction-cics https://www.ibm.com/support/pages/node/7171873
https://nvd.nist.gov/vuln/detail/CVE-2024-47100	7.1	Siemens products (SIMATIC S7 products)	Cross-Site Request Forgery (CSRF)	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-717113.html

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2024-55591 Fortinet FortiOS Authorization Bypass Vulnerability CVE-2025-21333 Microsoft Windows Hyper-V NT Kernel Integration VSP Heap-based Buffer Overflow Vulnerability CVE-2025-21334 Microsoft Windows Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability CVE-2025-21335 Microsoft Windows Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability CVE-2024-50603 Aviatrix Controllers OS Command Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2025/01/14/cisa-adds-four-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2025/01/16/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Industrial Control Systems Advisories	ICSA-25-014-01 Hitachi Energy FOXMAN-UN ICSA-25-014-02 Schneider Electric Vijeo Designer ICSA-25-014-03 Schneider Electric EcoStruxure ICSA-25-014-04 Belledonne Communications Linphone-Desktop ICSA-25-016-01 Siemens Mendix LDAP ICSA-25-016-02 Siemens Industrial Edge Management ICSA-25-016-03 Siemens Siveillance Video Camera ICSA-25-016-04 Siemens SIPROTEC 5 Products ICSA-25-016-05 Fuji Electric Alpha5 SMART ICSA-25-016-06 Hitachi Energy FOX61x, FOXCST, and FOXMAN-UN Products ICSA-25-016-07 Hitachi Energy FOX61x Products ICSA-25-016-08 Schneider Electric Data Center Expert ICSA-24-058-01 Mitsubishi Electric Multiple Factory Automation Products (Update A) ICSA-25-010-03 Delta Electronics DRASimuCAD (Update A) ICSA-24-191-05 Johnson Controls Inc. Software House C●CURE 9000 (Update A) ICSA-24-030-02 Mitsubishi Electric FA Engineering Software Products (Update B)	https://www.cisa.gov/news-events/alerts/2025/01/14/cisa-releases-four-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2025/01/16/cisa-releases-twelve-industrial-control-systems-advisories
Fortinet Releases Security Updates for Multiple Products	Fortinet Security Updates	https://www.cisa.gov/news-events/alerts/2025/01/14/fortinet-releases-security-updates-multiple-products
Ivanti Releases Security Updates for Multiple Products	Ivanti Avalanche Ivanti Application Control Engine Ivanti EPM	https://www.cisa.gov/news-events/alerts/2025/01/14/ivanti-releases-security-updates-multiple-products

Microsoft Releases January 2025 Security Updates	Microsoft Security Update Guide for January	https://www.cisa.gov/news-events/alerts/2025/01/14/microsoft-releases-january-2025-security-updates
Adobe Releases Security Updates for Multiple Products	Adobe Product Security Updates for January	https://www.cisa.gov/news-events/alerts/2025/01/14/adobe-releases-security-updates-multiple-products
Vulnerability Summary for the Week of January 6, 2025		https://www.cisa.gov/news-events/bulletins/sb25-013
CISA Releases Microsoft Expanded Cloud Logs Implementation Playbook	Microsoft Expanded Cloud Logs Implementation Playbook	https://www.cisa.gov/news-events/alerts/2025/01/15/cisa-releases-microsoft-expanded-cloud-logs-implementation-playbook

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
Fortinet fixes FortiOS zero-day exploited by attackers for months (CVE-2024-55591)	https://www.helpnetsecurity.com/2025/01/14/fortinet-fortigate-zero-day-vulnerability-exploited-cve-2024-55591/
New Hacking Group Leaks Configuration of 15,000 Fortinet Firewalls	https://www.infosecurity-magazine.com/news/hacking-group-leaks-config-15k/
159-CVE January Patch Tuesday smashes single-month record	https://news.sophos.com/en-us/2025/01/14/159-cve-january-patch-tuesday-smashes-single-month-record/
DORA Takes Effect: Financial Firms Still Navigating Compliance Headwinds	https://www.infosecurity-magazine.com/news/dora-financial-firms-compliance/
EU takes decisive action on healthcare cybersecurity	https://www.helpnetsecurity.com/2025/01/17/eu-action-plan-healthcare-cybersecurity/
GDPR complaints filed against TikTok, Temu for sending user data to China	https://www.bleepingcomputer.com/news/security/gdpr-complaints-filed-against-tiktok-temu-for-sending-user-data-to-china/
New Hacking Group Leaks Configuration of 15,000 Fortinet Firewalls	https://www.infosecurity-magazine.com/news/hacking-group-leaks-config-15k/
Researchers Warn of NTLMv1 Bypass in Active Directory Policy	https://hackread.com/researchers-ntlmv1-bypass-active-directory-policy/
Researcher Uncovers Critical Flaws in Multiple Versions of Ivanti Endpoint Manager	https://thehackernews.com/2025/01/researcher-uncovers-critical-flaws-in.html
Microsoft ends support for Office apps on Windows 10 in October	https://www.bleepingcomputer.com/news/microsoft/microsoft-ends-support-for-office-apps-on-windows-10-in-october/
FunkSec Ransomware Dominating Ransomware Attacks, Compromised 85 Victims in December	https://cybersecuritynews.com/funksec-ransomware-dominating-ransomware-attacks/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
183M Patient Records Exposed: Fortified Health Security Releases 2025 Healthcare Cybersecurity Report	https://www.darkreading.com/cyberattacks-data-breaches/183m-patient-records-exposed-fortified-health-security-releases-2025-healthcare-cybersecurity-report

Clop Ransomware exploits Cleo File Transfer flaw: dozens of claims, disputed breaches	https://securityaffairs.com/173135/cyber-crime/clop-ransomware-gang-claims-hack-of-cleo-file-transfer-customers.html

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Fortinet Confirms Critical Zero-Day Vulnerability in Firewalls	https://www.infosecurity-magazine.com/news/fortinet-confirms-critical-zero-day/
Over 660,000 Rsync servers exposed to code execution attacks	https://www.bleepingcomputer.com/news/security/over-660-000-rsync-servers-exposed-to-code-execution-attacks/
Google OAuth Vulnerability Exposes Millions via Failed Startup Domains	https://thehackernews.com/2025/01/google-oauth-vulnerability-exposes.html
CVE-2024–49113 “LDAP Nightmare”: First PoC Exploit of 2025 Targets Critical Windows Vulnerability	https://medium.com/@cyfernest/urgent-first-poc-exploit-of-2025-targets-critical-windows-vulnerability-cve-2024-49113-ldap-5f14fe37249a
W3 Total Cache plugin flaw exposes 1 million WordPress sites to attacks	https://www.bleepingcomputer.com/news/security/w3-total-cache-plugin-flaw-exposes-1-million-wordpress-sites-to-attacks/
4.2 million internet hosts hijacked via bugs in tunneling protocols	https://www.scworld.com/news/4-2-million-internet-hosts-hijacked-via-bugs-in-tunneling-protocols
New UEFI Secure Boot flaw exposes systems to bootkits, patch now	https://www.bleepingcomputer.com/news/security/new-uefi-secure-boot-flaw-exposes-systems-to-bootkits-patch-now/
Critical SimpleHelp vulnerabilities fixed, update your server instances!	https://www.helpnetsecurity.com/2025/01/16/critical-simplehelp-vulnerabilities-fixed-security-update-remote-support/
SAP fixes critical vulnerabilities in NetWeaver application servers	https://www.bleepingcomputer.com/news/security/sap-fixes-critical-vulnerabilities-in-netweaver-application-servers/
CVE-2024-44243 macOS flaw allows persistent malware installation	https://securityaffairs.com/173082/hacking/apple-macos-system-integrity-protection-sip-flaw.html
100 Million macOS Users At Risk – New Banshee Malware Attacks Bypassing Apple’s Xprotect	https://cybersecuritynews.com/banshee-malware-targets-macos/
Veeam Azure Backup Solution Vulnerability Allows Attackers To Enumerate Network	https://cybersecuritynews.com/veeam-azure-backup-solution-vulnerability/
Palo Alto Networks Expedition Tool Vulnerability Exposes Cleartext Firewall Passwords	https://cybersecuritynews.com/palo-alto-networks-expedition-firewall-passwords/
Cisco Releases Security Updates Addressing Vulnerabilities in ThousandEyes and Snort	https://cybersecuritynews.com/cisco-releases-security-updates/
Zoom Patches Multiple Vulnerabilities That Let Attackers Escalate Privileges	https://cybersecuritynews.com/zoom-matches-multiple-vulnerabilities/
Windows Line Printer Daemon (LPD) Vulnerability Exposes Systems to Remote Code Execution	https://cybersecuritynews.com/windows-lpd-vulnerability/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Thousands of WordPress sites impacted by WP3.XYZ malware campaign	https://www.scworld.com/brief/thousands-of-wordpress-sites-impacted-by-wp3-xyz-malware-campaign
Pro-Russian Hacker Group Targets Italian Banks and Public Services in DDoS Attacks	https://dailysecurityreview.com/security-spotlight/pro-russian-hacker-group-cyberattacks-on-italian-banks-and-public-services-in-ddos-attacks/
Ransomware Attack Paralyzes Slovakian Land Registry, Souring Slovakia-Ukraine Relations	https://dailysecurityreview.com/security-spotlight/slovakian-land-registry-cyberattack/
New 'Sneaky 2FA' Phishing Kit Targets Microsoft 365 Accounts with 2FA Code Bypass	https://thehackernews.com/2025/01/new-sneaky-2fa-phishing-kit-targets.html
Russia-linked APT Star Blizzard targets WhatsApp accounts	https://securityaffairs.com/173165/apt/russia-star-blizzard-targets-whatsapp-accounts.html
Russian APT Phishes Kazakh Gov't for Strategic Intel	https://www.darkreading.com/cyberattacks-data-breaches/russian-apt-phishes-kazakh-govt-strategic-intel
Malware spread by stealthy new MiktroTik botnet	https://www.scworld.com/brief/malware-spread-by-stealthy-new-miktrotik-botnet
Pumakit – A Sophisticated Linux Rootkit Attack Critical Infrastructure	https://cybersecuritynews.com/pumakit-linux-rootkit/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
New infosec products of the week: January 17, 2025	https://www.helpnetsecurity.com/2025/01/17/new-infosec-products-of-the-week-january-17-2025/

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/