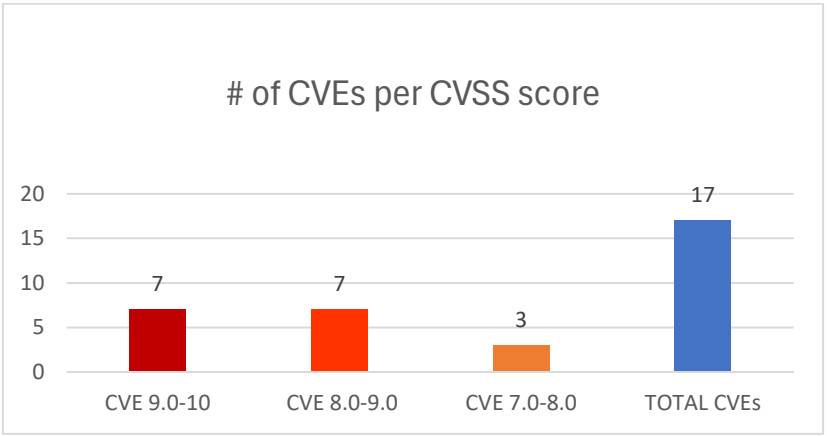
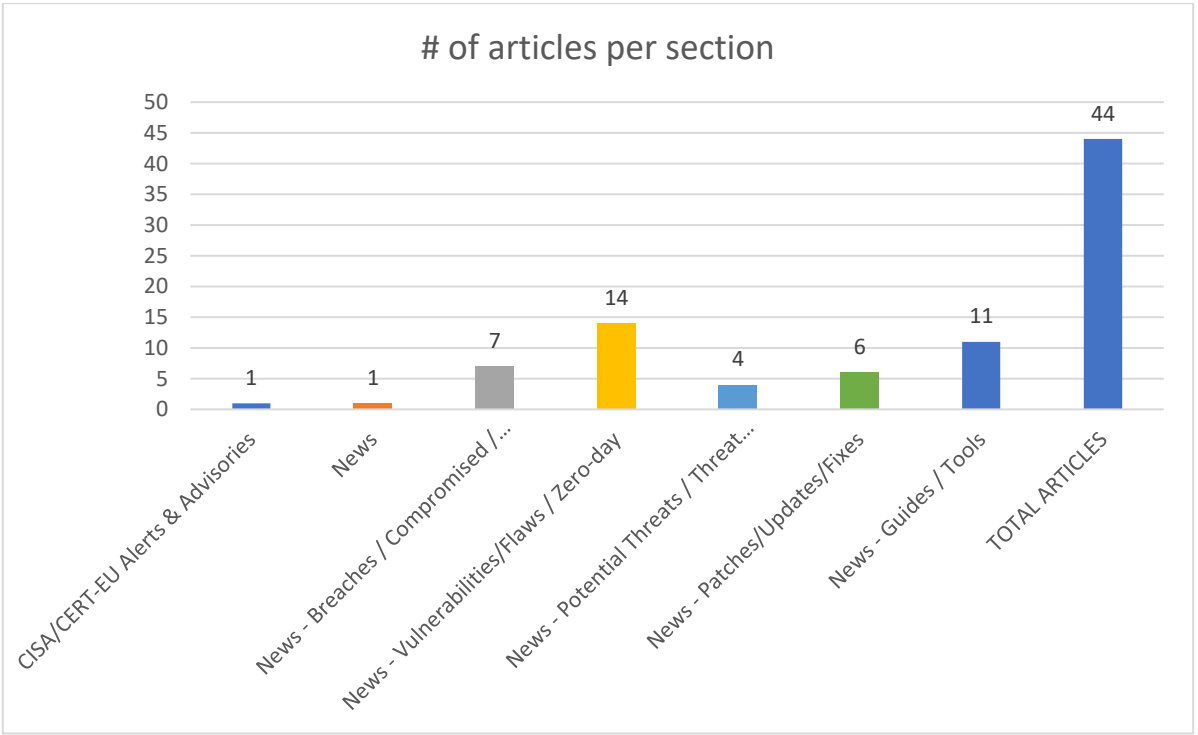
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 13/05/2026 - 15/05/2026





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-2026-44643	10,0	Angular Expressions	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	Prior to 1.5.2	https://github.com/peerigon/angular-expressions/security/advisories/GHSA-pw8r-6689-xvf4
https://nvd.nist.gov/vuln/detail/CVE-2026-8181	9,8	The Burst Statistics – Privacy-Friendly WordPress Analytics (Google Analytics Alternative) plugin for WordPress	Improper Authentication	3.4.0 to 3.4.1.1	https://github.com/Burst-Statistics/burst-statistics/blob/2488d3fa54045e7e5342b0445b9f6b5eaac9ea7c/includes/Frontend/class-mainwp-proxy.php#L385 Wordfence https://plugins.trac.wordpress.org/browser/burst-statistics/tags/3.4.1.1/includes/Frontend/class-mainwp-proxy.php#L314 Wordfence https://plugins.trac.wordpress.org/browser/burst-statistics/tags/3.4.1.1/includes/Frontend/class-mainwp-proxy.php#L328 Wordfence https://plugins.trac.wordpress.org/browser/burst-statistics/tags/3.4.1.1/includes/Frontend/class-mainwp-proxy.php#L336 Wordfence https://plugins.trac.wordpress.org/browser/burst-statistics/tags/3.4.1.1/includes/Traits/trait-admin-helper.php#L205 Wordfence https://plugins.trac.wordpress.org/browser/burst-statistics/trunk/includes/Frontend/class-mainwp-proxy.php#L314 Wordfence https://plugins.trac.wordpress.org/browser/burst-statistics/trunk/includes/Frontend/class-mainwp-proxy.php#L328 Wordfence https://plugins.trac.wordpress.org/browser/burst-statistics/trunk/includes/Frontend/class-mainwp-proxy.php#L336 Wordfence

					https://plugins.trac.wordpress.org/browser/burst-statistics/trunk/includes/Traits/trait-admin-helper.php#L205 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/8ca830d6-3d3c-4026-85cd-8447b8a568d3?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-6510	9,8	The InfusedWoo Pro plugin for WordPress	Missing Authorization	up to, and including, 5.1.2	https://woo.infusedaddons.com/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/08cb8ba1-1976-438b-8e0b-0a8be08aad6c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-6271	9,8	The Career Section plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.7	https://plugins.trac.wordpress.org/changeset/3507785/career-section Wordfence https://plugins.trac.wordpress.org/changeset/3507912/career-section Wordfence https://plugins.trac.wordpress.org/changeset/3507917/career-section Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/005d1abc-761d-4f9a-bc21-aad63e8efd66?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-8043	9,6	Ivanti Xtraction	External Control of File Name or Path	before version 2026.2	https://hub.ivanti.com/s/article/Security-Advisory---Ivanti-Xtraction-CVE-2026-8043?language=en_US
https://nvd.nist.gov/vuln/detail/CVE-2026-45714	9,1	CubeCart	Improper Control of Generation of Code ('Code Injection')	Prior to 6.7.0	https://github.com/cubecart/v6/security/advisories/GHSA-pcfr-xgc9-xfv6
https://nvd.nist.gov/vuln/detail/CVE-2026-45158	9,1	OPNsense is a FreeBSD	Improper Neutralization of Argument	Prior to 26.1.8	https://github.com/opnsense/core/security/advisories/GHSA-5rx3-w735-74wm

			Delimiters in a Command ('Argument Injection')		
https://nvd.nist.gov/vuln/detail/CVE-2026-8201	8,8	MongoDB's Field-Level Encryption (FLE)	Use After Free	v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2	https://jira.mongodb.org/browse/SERVER-122032
https://nvd.nist.gov/vuln/detail/CVE-2026-43908	8,8	OpenImageIO	Out-of-bounds Write	Prior to 3.0.18.0 and 3.1.13.0	https://github.com/AcademySoftwareFoundation/OpenImageIO/security/advisories/GHSA-2jr5-q49v-3858
https://nvd.nist.gov/vuln/detail/CVE-2020-37221	8,4	Atomic Alarm Clock	Stack-based Buffer Overflow	6.3	https://www.exploit-db.com/exploits/48346 VulnCheck https://www.vulncheck.com/advisories/atomic-alarm-clock-stack-overflow-via-seh-unicode
https://nvd.nist.gov/vuln/detail/CVE-2026-40893	8,2	Gotenberg is a Docker-powered	External Control of File Name or Path	Prior to 8.31.0	Source(s) Tag(s) https://github.com/gotenberg/gotenberg/security/advisories/GHSA-62p3-hvxx-fxg4
https://nvd.nist.gov/vuln/detail/CVE-2026-8629	8,1	Crabbox	Authorization Bypass Through User-Controlled Key	prior to v0.12.0	https://github.com/openclaw/crabbox/commit/95cb30dc7dbaa1fef690a42ef6ac1cb6e307a191 VulnCheck https://github.com/openclaw/crabbox/pull/71 CISA-ADP, VulnCheck https://github.com/openclaw/crabbox/releases/tag/v0.12.0 VulnCheck

					https://www.vulncheck.com/advisories/crabbox-privilege-escalation-via-agent-ticket-endpoints
https://nvd.nist.gov/vuln/detail/CVE-2026-44574	8,1	Next.js	Authentication Bypass Using an Alternate Path or Channel	From 15.4.0 to before 15.5.16 and 16.2.5	https://github.com/vercel/next.js/security/advisories/GHSA-492v-c6pp-mqqv
https://nvd.nist.gov/vuln/detail/CVE-2026-42897	8,1	Microsoft Exchange Server	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897
https://nvd.nist.gov/vuln/detail/CVE-2026-44447	7,5	ERPNext	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Prior to 16.9.0	https://github.com/frappe/erpnext/security/advisories/GHSA-q65v-fm9p-9vh3
https://nvd.nist.gov/vuln/detail/CVE-2026-41218	7,5	BIG-IP PEM iRules	Use After Free		https://my.f5.com/manage/s/article/K000160875
https://nvd.nist.gov/vuln/detail/CVE-2026-8597	7,2	Triton inference handler in Amazon SageMaker Python SDK	Improper Validation of Integrity Check Value	v2 before v2.257.2 and v3 before v3.8.0	https://aws.amazon.com/security/security-bulletins/2026-031-aws/ AMZN https://github.com/aws/sagemaker-python-sdk/releases/tag/v2.257.2 AMZN https://github.com/aws/sagemaker-python-sdk/releases/tag/v3.8.0 AMZN https://github.com/aws/sagemaker-python-sdk/security/advisories/GHSA-rq6v-x3j8-7qgf

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-2026-20182 Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/05/14/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
Taiwan Incident Highlights Cybersecurity Gaps in Rail Systems	https://www.darkreading.com/ics-ot-security/taiwan-incident-highlights-cybersecurity-gaps

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
Foxconn Confirms Cyberattack After Nitrogen Ransomware Gang Claim	https://cybersecuritynews.com/foxconn-confirms-cyberattack/
Tables Turn on 'The Gentlemen' RaaS Gang With Data Leak	https://www.darkreading.com/threat-intelligence/gentlemen-raas-gang-data-leak
Avada Builder Flaws Expose One Million WordPress Sites	https://www.infosecurity-magazine.com/news/avada-builder-flaws-one-million/
Chinese APT Hackers Exploit Microsoft Exchange to Breach Energy Sector Network	https://cybersecuritynews.com/chinese-apt-hackers-exploit-microsoft-exchange/
node-ipc npm Package with 822K Weekly Downloads Compromised in Supply Chain Attack	https://cybersecuritynews.com/node-ipc-npm-package-compromised/
Hackers Compromise 170 npm Packages to Steal GitHub, npm, AWS, and Kubernetes Secrets	https://cybersecuritynews.com/hackers-compromise-170-npm-packages/
OpenAI Confirms Security Breach Via TanStack npm Supply Chain Attack	https://cybersecuritynews.com/openai-confirms-security-breach/

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 18-Year-Old NGINX Vulnerability Enables Remote Code Execution Attacks – PoC Released	https://cybersecuritynews.com/18-year-old-nginx-rce-vulnerability/
Critical MongoDB Vulnerability Allow Attackers to Execute Arbitrary Code	https://cybersecuritynews.com/mongodb-rce-vulnerability/
Windows BitLocker 0-Day Vulnerability Enables Access to Encrypted Drives	https://cybersecuritynews.com/windows-bitlocker-0-day-vulnerability/
Microsoft Teams Vulnerability Allows Hackers to Perform Spoofing Attacks	https://cybersecuritynews.com/microsoft-teams-vulnerability-spoofing/
New Exim BDAT GnuTLS Vulnerability Enables Code Execution Attacks	https://cybersecuritynews.com/new-exim-bdat-gnutls-vulnerability/
Critical SandboxJS Escape Vulnerability Enables Host Takeover	https://cybersecuritynews.com/critical-sandboxjs-escape-vulnerability/
Fragnesia Linux Vulnerability Let Attackers Gain Root Privileges – PoC Released	https://cybersecuritynews.com/fragnesia-linux-vulnerability/
Microsoft, Palo Alto Networks Find Many Vulnerabilities by Using AI on Their Own Code	https://www.securityweek.com/microsoft-palo-alto-networks-find-many-vulnerabilities-by-using-ai-on-their-own-code/
On-Prem Microsoft Exchange Server CVE-2026-42897 Exploited via Crafted Email	https://thehackernews.com/2026/05/on-prem-microsoft-exchange-server-cve.html
CISA Adds Cisco SD-WAN CVE-2026-20182 to KEV After Admin Access Exploits	https://thehackernews.com/2026/05/cisa-adds-cisco-sd-wan-cve-2026-20182.html
New Linux Kernel Vulnerability Fragnesia Allows Root Privilege Escalation	https://www.securityweek.com/new-linux-kernel-vulnerability-fragnesia-allows-root-privilege-escalation/
Hackers exploit auth bypass flaw in Burst Statistics WordPress plugin	https://www.bleepingcomputer.com/news/security/hackers-exploit-auth-bypass-flaw-in-burst-statistics-wordpress-plugin/
18-year-old NGINX vulnerability allows DoS, potential RCE	https://www.bleepingcomputer.com/news/security/18-year-old-nginx-vulnerability-allows-dos-potential-rce/
Critical Canon MailSuite Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/canon-mailsuite-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
Microsoft Releases Cumulative Update for Windows 11, Version 25H2 and 24H2	https://cybersecuritynews.com/microsoft-releases-cumulative-update-for-windows-11/
Microsoft Patches 138 Vulnerabilities, Including DNS and Netlogon RCE Flaws	https://thehackernews.com/2026/05/microsoft-patches-138-vulnerabilities.html
Microsoft's MDASH AI System Finds 16 Windows Flaws Fixed in Patch Tuesday	https://thehackernews.com/2026/05/microsofts-mdash-ai-system-finds-16.html
Chrome 148 Update Patches Critical Vulnerabilities	https://www.securityweek.com/chrome-148-update-patches-critical-vulnerabilities/
Cisco Patches Another SD-WAN Zero-Day, the Sixth Exploited in 2026	https://www.securityweek.com/cisco-patches-another-sd-wan-zero-day-the-sixth-exploited-in-2026/

F5 Patches Over 50 Vulnerabilities	https://www.securityweek.com/f5-patches-over-50-vulnerabilities/

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
ClickFix Evolves with 10-Year-Old Open-Source Python SOCKS5 Proxy	https://cybersecuritynews.com/clickfix-evolves-with-python-socks5-proxy/
China-Linked Hackers Deploy New TencShell Malware Against Global Manufac-turer	https://www.infosecurity-magazine.com/news/china-hackers-tencshell-malware/
Hackers Abuse Scheduled Tasks to Maintain Persistence in FrostyNeighbor Attacks	https://cybersecuritynews.com/hackers-abuse-scheduled-tasks-to-maintain-persistence/
New Malware Framework Enables Screen Control, Browser Artifact Access, and UAC Bypass	https://cybersecuritynews.com/new-malware-framework-enables-screen-control/

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/**
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/