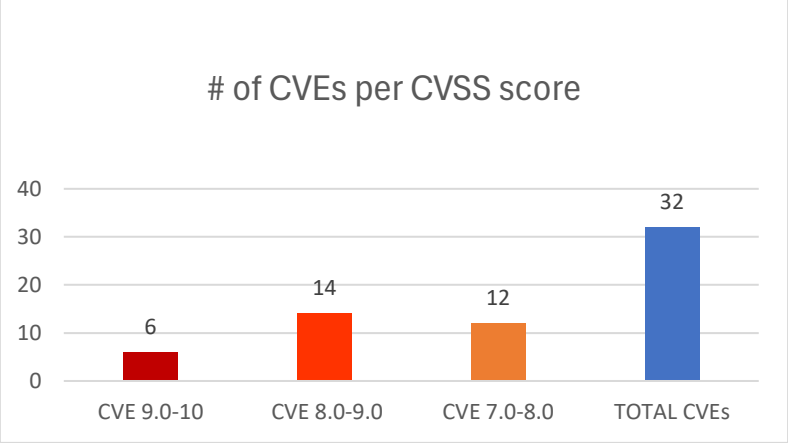
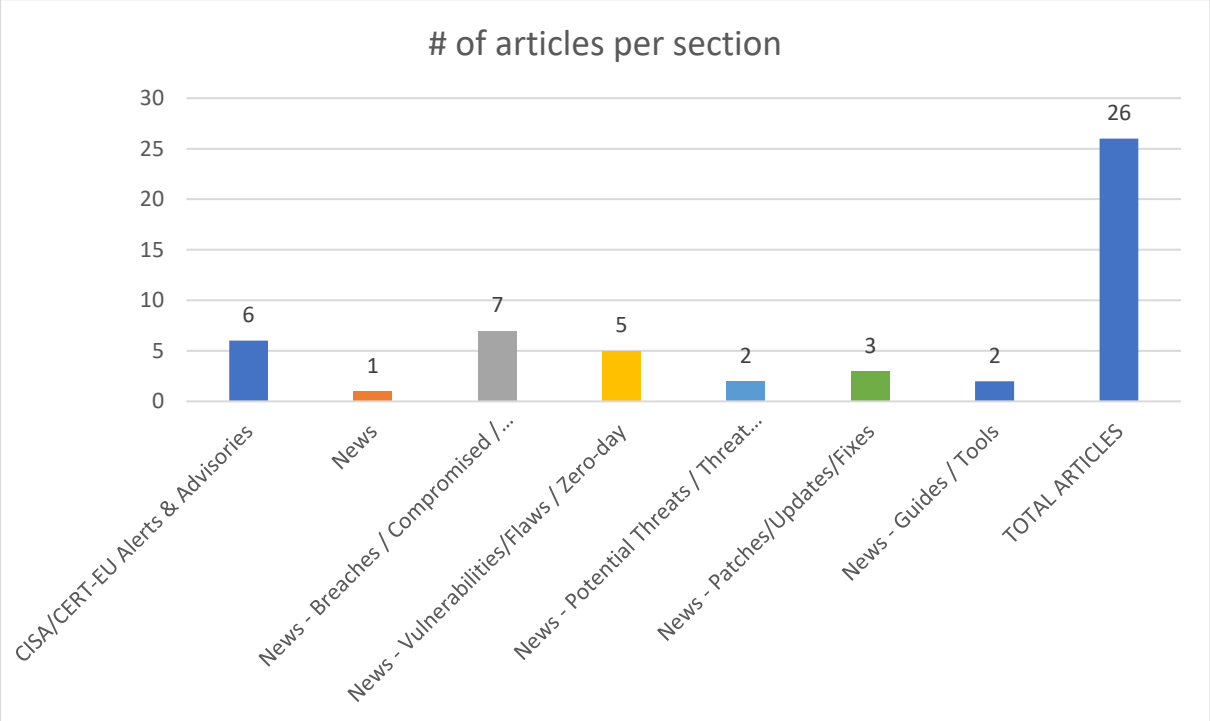
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 06/08/2025 - 08/08/2025





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-2025-53767	10,0	Azure OpenAI Elevation	Server-Side Request Forgery (SSRF)		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53767
https://nvd.nist.gov/vuln/detail/CVE-2025-6994	9,8	The Reveal Listing plugin by smartdatasoft for WordPress	Improper Privilege Management	versions up to, and including, 3.3	https://themeforest.net/item/reveal-directory-listing-wordpress-theme/27704330 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/cd00d716-535c-41eb-a766-82079e0060e6?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-23310	9,8	NVIDIA Triton Inference Server for Windows and Linux	Stack-based Buffer Overflow		https://nvd.nist.gov/vuln/detail/CVE-2025-23310 NVIDIA Corporation https://nvidia.custhelp.com/app/answers/detail/a_id/5687 NVIDIA Corporation https://www.cve.org/CVERecord?id=CVE-2025-23310
https://nvd.nist.gov/vuln/detail/CVE-2025-30127	9,8	Marbella KR8s Dashcam FF	Improper Access Control	2.0.8	https://geochen.medium.com/marbella-dashcam-ab40ca41adec MITRE https://github.com/geo-chen/Marbella/ MITRE https://github.com/geo-chen/Marbella/blob/main/README.md#finding-2---cve-2025-30127-video-recordings-open-to-being-downloaded-via-ports-7777-7778-7779 MITRE https://makagps.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-54594	9,1	react-native-bottom-tabs is a library of Native Bottom Tabs for React Native	Improper Privilege Management	versions 0.9.2 and below	https://callstack.notion.site/Post-Incident-Security-Measures-GitHub-Actions-Workflow-Vulnerability-2405d027c0f8804ab7f7cdfb43366a31 GitHub, Inc. https://github.com/callstackincubator/react-native-bottom-tabs/commit/9e1c9c61d742c435ac5e0901b7e0c9249b9fc70c GitHub, Inc. https://github.com/callstackincubator/react-native-bottom-tabs/security/advisories/GHSA-588g-38p4-gr6x
https://nvd.nist.gov/vuln/detail/CVE-2025-53792	9,1	Azure Portal Elevation	Improper Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53792

https://nvd.nist.gov/vuln/detail/CVE-2025-8653	8,8	Kenwood DMX958XR JKRadioService	Stack-based Buffer Overflow		https://www.zerodayinitiative.com/advisories/ZDI-25-801/
https://nvd.nist.gov/vuln/detail/CVE-2025-54785	8,8	SuiteCRM	Improper Input Validation	In versions 7.14.6 and 8.8.0	https://docs.suitecrm.com/admin/releases/7.14.x/#_7_14_7 GitHub, Inc. https://github.com/SuiteCRM/SuiteCRM/security/advisories/GHSA-53cp-mpfw-qj67
https://nvd.nist.gov/vuln/detail/CVE-2025-51629	8,8	PdfViewer component of Agenzia Impresa Eccobook	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2.81.1	http://agenzia.com MITRE http://eccobook.com MITRE https://github.com/CapgeminiCisRedTeam/Disclosure/blob/main/CVE%20PoC/CVE-2025-51629%20%7C%20Eccobook.md
https://nvd.nist.gov/vuln/detail/CVE-2023-41532	8,8	Hospital Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	v4	https://gist.github.com/celbahraoui/9972727c6770cd63386ebbe07a9c1454 MITRE https://github.com/kishan0725/Hospital-Management-System
https://nvd.nist.gov/vuln/detail/CVE-2023-41520	8,8	Student Attendance Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	v1	https://gist.github.com/celbahraoui/39c19c0b7f9f92a1a7e06d1c928bb1c3 MITRE https://github.com/rickxy/Student-Attendance-Management-System
https://nvd.nist.gov/vuln/detail/CVE-2025-24000	8,8	WPExperts Post SMTP	Authentication Bypass Using an Alternate Path or Channel	from n/a through 3.2.0	https://patchstack.com/database/wordpress/plugin/post-smtp/vulnerability/wordpress-post-smtp-3-2-0-privilege-escalation-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-8578	8,8	Cast in Google Chrome	Use After Free	prior to 139.0.7258.66	https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop.html Chrome https://issues.chromium.org/issues/423387026
https://nvd.nist.gov/vuln/detail/CVE-2025-54886	8,4	skops is a Python library	Deserialization of Untrusted Data	In versions 0.12.0	https://github.com/skops-dev/skops/commit/29d61ea8a92f2bde6830e8f32cc72a1a87211cda GitHub, Inc. https://github.com/skops-dev/skops/security/advisories/GHSA-378x-6p4f-8jgm

https://nvd.nist.gov/vuln/detail/CVE-2025-6633	8,3	Autodesk 3ds Max	Out-of-bounds Write		https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0016
https://nvd.nist.gov/vuln/detail/CVE-2025-53787	8,2	Microsoft 365 Copilot BizChat	Improper Neutralization of Special Elements used in a Command ('Command Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53787
https://nvd.nist.gov/vuln/detail/CVE-2025-8420	8,1	The Request a Quote Form plugin for WordPress	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	version less than, or equal to, 2.5.2	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3338854%40request-a-quote&new=3338854%40request-a-quote&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/601aa2b5-aeac-49bc-960d-4b4ff83e9229?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3320	8,1	IBM Tivoli Monitoring	Heap-based Buffer Overflow	6.3.0.7 through 6.3.0.7	https://www.ibm.com/support/pages/node/7241472
https://nvd.nist.gov/vuln/detail/CVE-2025-50286	8,1	Grav CMS	Unrestricted Upload of File with Dangerous Type	v1.7.48	https://github.com/binneko/CVE-2025-50286
https://nvd.nist.gov/vuln/detail/CVE-2025-53786	8,0	Microsoft Exchange server	Improper Authentication		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53786
https://nvd.nist.gov/vuln/detail/CVE-2025-38747	7,8	Dell SupportAssist OS Recovery	Creation of Temporary File With Insecure Permissions	versions prior to 5.5.14.0	https://www.dell.com/support/kbdoc/en-us/000353093/dsa-2025-315
https://nvd.nist.gov/vuln/detail/CVE-2025-51624	7,6	Zone Bitaqati	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	3.4.0	http://bitaqati.com MITRE http://zone.com MITRE https://medium.com/@a77777mad/cross-site-scripting-xss-vulnerability-in-zone-bitaqati-v3-4-0-a05b980b4df4 MITRE https://zone.net.sa/bitaqati-self-service/

https://nvd.nist.gov/vuln/detail/CVE-2025-7036	7,5	The CleverReach® WP plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 1.5.20	https://plugins.trac.wordpress.org/browser/cleverreach-wp/tags/1.5.20/Controllers/class-clever-reach-article-search-controller.php#L159 Wordfence https://wordpress.org/plugins/cleverreach-wp/#developers Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/764041ca-65cd-498c-97e5-a33d7b54a2b9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-51532	7,5	Sage DPW	Improper Access Control	v2024.12.003	https://www.sec4you-pentest.com/schwachstelle/sage-dpw-unauthentifizierter-zugriff-adminbereich-db-monitor/ MITRE https://www.sec4you-pentest.com/schwachstellen/
https://nvd.nist.gov/vuln/detail/CVE-2025-46659	7,5	ExonautWeb in 4C Strategies Exonaut	Exposure of Sensitive Information to an Unauthorized Actor	21.6	https://gist.github.com/Jowu73/a393a8de99f2dbefcca7d9727c412dff MITRE https://www.4cstrategies.com/solutions/exonaut/
https://nvd.nist.gov/vuln/detail/CVE-2025-35970	7,5	SEIKO EPSON and FUJIFILM Corporation	Use of Weak Credentials		https://global.fujifilm.com/en/news/hq/697e JPCERT/CC https://jvn.jp/en/vu/JVNVU91363496/ JPCERT/CC https://www.epson.jp/support/misc_t/250807_oshirase.htm
https://nvd.nist.gov/vuln/detail/CVE-2025-55077	7,4	Tyler Technologies ERP Pro 9 SaaS	Incorrect Authorization		https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2025/va-25-219-01.json Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government https://www.cve.org/CVERecord?id=CVE-2025-55077
https://nvd.nist.gov/vuln/detail/CVE-2025-55137	7,4	LinkJoin	Access of Resource Using Incompatible Type ('Type Confusion')	through 882f196	https://github.com/Latkecrszy/linkjoin/pull/4
https://nvd.nist.gov/vuln/detail/CVE-2025-22469	7,3	CL4/6NX Plus and CL4/6NX-J Plus (Japan model)	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	versions prior to 1.15.5-r1	https://jvn.jp/en/jp/JVN16547726/ JPCERT/CC https://www.sato-global.com/support_notices/240830/

https://nvd.nist.gov/vuln/detail/CVE-2025-54882	7,1	**Himmelblau suite for Microsoft Azure Entra ID and Intune**	Insufficiently Protected Credentials	versions 0.8.0 through 0.9.21 and 1.0.0-beta through 1.1.0	https://github.com/himmelblau-idm/himmelblau/commit/b562053df3dffb1dd9ab3d09af986886773be2ad GitHub, Inc. https://github.com/himmelblau-idm/himmelblau/commit/faae58b0384aca8b21b4be5f1c507412eec3778a GitHub, Inc. https://github.com/himmelblau-idm/himmelblau/releases/tag/0.9.22 GitHub, Inc. https://github.com/himmelblau-idm/himmelblau/releases/tag/1.2.0 GitHub, Inc. https://github.com/himmelblau-idm/himmelblau/security/advisories/GHSA-phfx-rjfw-wj83
https://nvd.nist.gov/vuln/detail/CVE-2025-3770	7,0	EDK2	Protection Mechanism Failure		https://github.com/tianocore/edk2/security/advisories/GHSA-vx5v-4gg6-6qxr
https://nvd.nist.gov/vuln/detail/CVE-2025-26513	7,0	SAN Host Utilities for Windows		versions prior to 8.0	https://security.netapp.com/advisory/NTAP-20250806-0001

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Microsoft Releases Guidance on High-Severity Vulnerability (CVE-2025-53786) in Hybrid Exchange Deployments	CVE-2025-53786	https://www.cisa.gov/news-events/alerts/2025/08/06/microsoft-releases-guidance-high-severity-vulnerability-cve-2025-53786-hybrid-exchange-deployments
CISA Releases Malware Analysis Report Associated with Microsoft SharePoint Vulnerabilities	▪ CVE-2025-49704 [CWE-94: Code Injection], ▪ CVE-2025-49706 [CWE-287: Improper Authentication], ▪ CVE-2025-53770 [CWE-502: Deserialization of Untrusted Data], and ▪ CVE-2025-53771 [CWE-287: Improper Authentication]	https://www.cisa.gov/news-events/alerts/2025/08/06/cisa-releases-malware-analysis-report-associated-microsoft-sharepoint-vulnerabilities
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2020-25078 D-Link DCS-2530L and DCS-2670L Devices Unspecified Vulnerability ▪ CVE-2020-25079 D-Link DCS-2530L and DCS-2670L Command Injection Vulnerability ▪ CVE-2022-40799 D-Link DNR-322L Download of Code Without Integrity Check Vulnerability	https://www.cisa.gov/news-events/alerts/2025/08/05/cisa-adds-three-known-exploited-vulnerabilities-catalog
CISA Releases Ten Industrial Control Systems Advisories	▪ ICSA-25-219-01 Delta Electronics DIAView ▪ ICSA-25-219-02 Johnson Controls FX80 and FX90 ▪ ICSA-25-219-03 Burk Technology ARC Solo ▪ ICSA-25-219-04 Rockwell Automation Arena ▪ ICSA-25-219-05 Packet Power EMX and EG ▪ ICSA-25-219-06 Dreame Technology iOS and Android Mobile Applications ▪ ICSA-25-219-07 EG4 Electronics EG4 Inverters ▪ ICSA-25-219-08 Yealink IP Phones and RPS (Redirect and Provisioning Service) ▪ ICSA-25-148-04 Instantel Micromate (Update A) ▪ ICSA-25-140-04 Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update A)	https://www.cisa.gov/news-events/alerts/2025/08/07/cisa-releases-ten-industrial-control-systems-advisories
CISA Issues ED 25-02: Mitigate Microsoft Exchange Vulnerability	CVE-2025-53786	https://www.cisa.gov/news-events/alerts/2025/08/07/cisa-issues-ed-25-02-mitigate-microsoft-exchange-vulnerability
CISA Releases Two Industrial Control Systems Advisories	▪ **ICSA-25-217-01 Mitsubishi Electric Iconics Digital Solutions Multiple Products** ▪ **ICSA-25-217-02 Tigo Energy Cloud Connect Advanced**	https://www.cisa.gov/news-events/alerts/2025/08/05/cisa-releases-two-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
CISA Releases Emergency Advisory Urges Feds to Patch Exchange Server Vulnerability by Monday	https://cybersecuritynews.com/cisa-exchange-server-advisory/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Clinical Data Stolen in Cyber-Attack on Kidney Dialysis Provider DaVita	https://www.infosecurity-magazine.com/news/clinical-data-stolen-kidney/
Hacker Accesses Millions of IMDataCenter Records from Exposed AWS Bucket	https://hackread.com/hacker-accesses-imdatacenter-records-exposed-aws-bucket/?&web_view=true
Ransomware gang gives Ridgefield Public Schools 2 days to pay before 90 GB is leaked	https://www.comparitech.com/news/ransomware-gang-gives-ridgefield-public-schools-2-days-to-pay-before-90-gb-is-leaked/?&web_view=true
KLM Confirms Customer Data Breach Linked to Third-Party System	https://hackread.com/klm-customer-data-breach-linked-third-party-system/?&web_view=true
Air France and KLM disclose data breaches impacting customers	https://www.bleepingcomputer.com/news/security/air-france-and-klm-disclose-data-breaches-impacting-customers/
Google confirms customer data stolen from Salesforce DB	https://www.theregister.com/2025/08/06/google_salesforce_attacks/?&web_view=true
PBS confirms data breach after employee info leaked on Discord servers	https://www.bleepingcomputer.com/news/security/pbs-confirms-data-breach-after-employee-info-leaked-on-discord-servers/?&web_view=true

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Discloses Exchange Server Flaw Enabling Silent Cloud Access in Hybrid Setups	https://thehackernews.com/2025/08/microsoft-discloses-exchange-server.html
Trend Micro Confirms Active Exploitation of Critical Apex One Flaws in On-Premise Systems	https://thehackernews.com/2025/08/trend-micro-confirms-active.html
ReVault flaws let hackers bypass Windows login on Dell laptops	https://www.bleepingcomputer.com/news/security/revault-flaws-let-hackers-bypass-windows-login-on-dell-laptops/
6,500 Axis Servers Expose Remoting Protocol; 4,000 in U.S. Vulnerable to Exploits	https://thehackernews.com/2025/08/6500-axis-servers-expose-remoting.html
CISA, Microsoft warn of critical Exchange hybrid flaw CVE-2025-53786	https://securityaffairs.com/180923/security/cisa-microsoft-warn-of-critical-exchange-hybrid-flaw-cve-2025-53786.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
SonicWall Confirms Patched Vulnerability Behind Recent VPN Attacks, Not a Zero-Day	https://thehackernews.com/2025/08/sonicwall-confirms-patched.html
Adobe Issues Out-of-Band Patches for AEM Forms Vulnerabilities With Public PoC	https://www.securityweek.com/adobe-issues-out-of-band-patches-for-aem-forms-vulnerabilities-with-public-poc/
Ox Security Launches AI Agent That Auto-Generates Code to Fix Vulnerabilities	https://www.securityweek.com/ox-security-launches-ai-agent-that-auto-generates-code-to-fix-vulnerabilities/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
WhatsApp Developers Under Attack From Weaponized npm Packages with Remote Kill Switch	https://cybersecuritynews.com/whatsapp-developers-under-attack/
Hackers Weaponizing SVG Files With Malicious Embedded JavaScript to Execute Malware on Windows Systems	https://cybersecuritynews.com/hackers-weaponizing-svg-files-with-malicious-embedded-javascript/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/
10 Best Vulnerability Management Tools In 2025	https://cybersecuritynews.com/vulnerability-management-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/