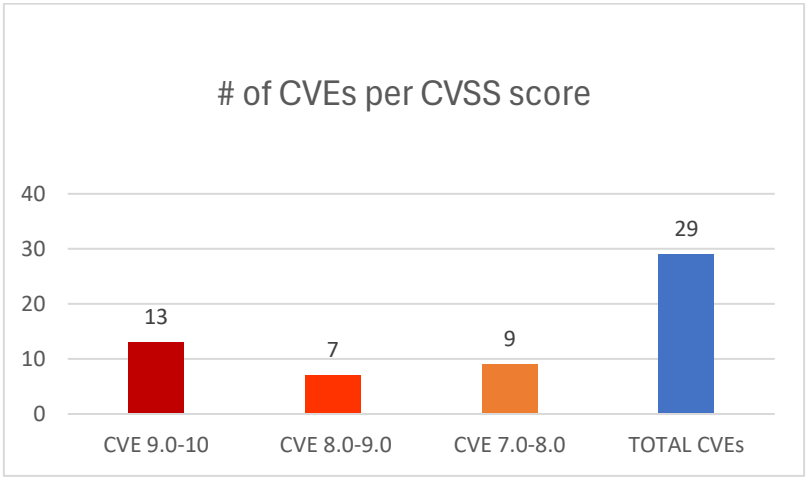
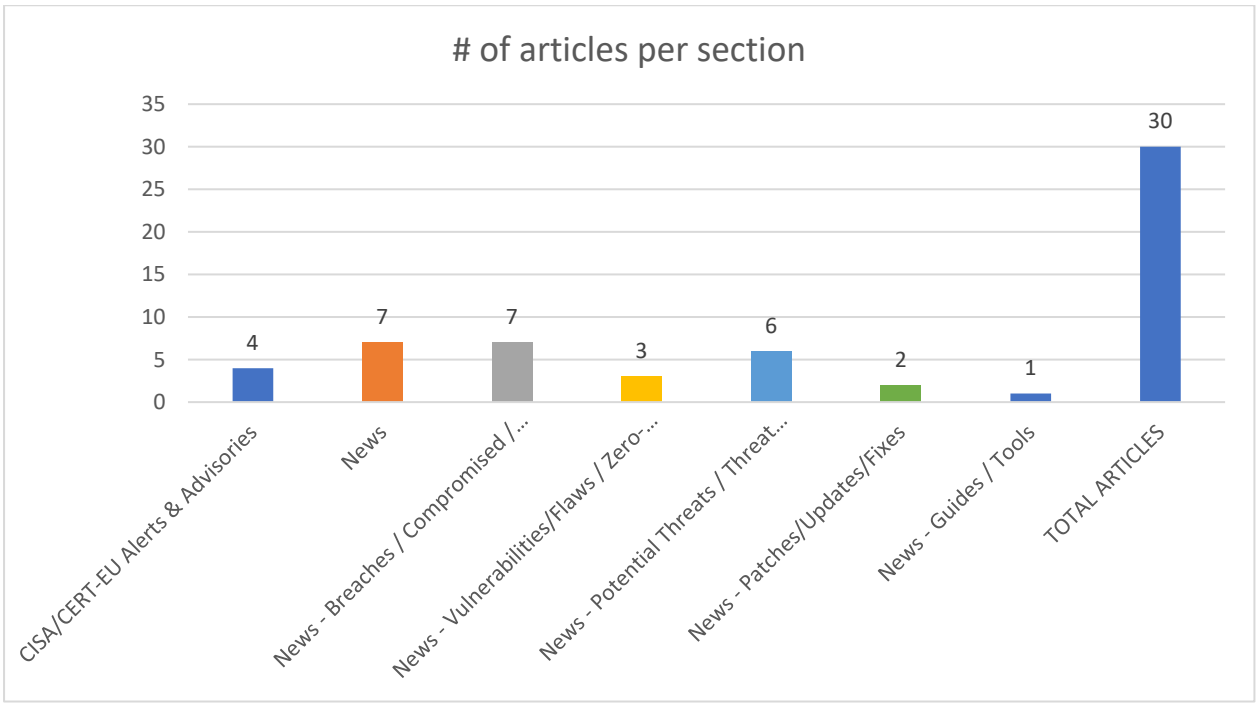

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

**Date: 28/05/2025 - 30/05/2025**



# 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-2025-32440 | 10,0 | NetAlertX | Missing Authentication for Critical Function | Prior to version 25.4.14 | https://github.com/jokob-sk/NetAlertX/releases/tag/v25.4.14 https://github.com/jokob-sk/NetAlertX/security/advisories/GHSA-h4x5-vr54-vjrx https://github.com/jokob-sk/NetAlertX/security/advisories/GHSA-h4x5-vr54-vjrx |
| https://nvd.nist.gov/vuln/detail/CVE-2025-48827 | 10,0 | vBulletin | Improper Protection of Alternate Path | vBulletin 5.0.0 through 5.7.5 and 6.0.0 through 6.0.3 | https://blog.kevintel.com/vbulletin-replaceadtemplate-kev/ https://karmainsecurity.com/dont-call-that-protected-method-vbulletin-rce https://kevintel.com/CVE-2025-48827 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-48748 | 10,0 | Netwrix Directory Manager | Use of Hard-coded Credentials | through v.10.0.7784.0 | https://community.netwrix.com/t/adv-2025-013-hard-coded-password-in-netwrix-directory-manager-formerly-imanami-groupid-v10-and-earlier/13945 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-22252 | 9,8 | Fortinet FortiProxy | Missing Authentication for Critical Function | Fortinet FortiProxy versions 7.6.0 through 7.6.1, FortiSwitchManager version 7.2.5, and FortiOS versions 7.4.4 through 7.4.6 and version 7.6.0 | https://fortiguard.fortinet.com/psirt/FG-IR-24-472 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-3357 | 9,8 | IBM Tivoli Monitoring | Improper Validation of Specified Index, Position, or Offset in Input | IBM Tivoli Monitoring 6.3.0.7 through 6.3.0.7 Service Pack 19 | https://www.ibm.com/support/pages/node/7234923 |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-45343 | 9,8 | Tenda W18E | Improper Access Control | Tenda W18E v.2.0 v.16.01.0.11 | http://w18e.com https://gist.github.com/isstabber/b363d47966965e5c0a8ec26d445e090b https://gist.github.com/isstabber/b363d47966965e5c0a8ec26d445e090b https://www.tenda.com.cn/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-48336 | 9,8 | ThimPress Course Builder | Deserialization of Untrusted Data | from n/a before 3.6.6 | https://patchstack.com/database/wordpress/theme/course-builder/vulnerability/wordpress-course-builder-3-6-6-php-object-injection-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2023-41591 | 9,8 | Open Network Foundation ONOS | Authentication Bypass by Spoofing | v2.7.0 | https://gist.github.com/kjw6855/9764e3f51b89119473e4d2c4f64dca27 https://wiki.onosproject.org/pages/viewpage.action?pageId=16122675 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-5277 | 9,6 | aws-mcp-server MCP server | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | aws-mcp-server MCP server | https://github.com/alexei-led/aws-mcp-server/blob/94d20ae1798a43ac7e3a28e71900d774e5159c8a/src/aws_mcp_server/cli_executor.py#L92 https://github.com/alexei-led/aws-mcp-server/commit/94d20ae1798a43ac7e3a28e71900d774e5159c8a |
| https://nvd.nist.gov/vuln/detail/CVE-2025-48749 | 9,1 | Netwrix Directory Manager (formerly Imanami GroupID) | Insertion of Sensitive Information Into Sent Data | Netwrix Directory Manager (formerly Imanami GroupID) v11.0.0.0 and before & after v.11.1.25134.03 | https://community.netwrix.com/t/adv-2025-014-critical-vulnerabilities-in-netwrix-directory-manager-formerly-imanami-groupid-v11/13951 https://netwrix.com |
| https://nvd.nist.gov/vuln/detail/CVE-2025-4967 | 9,1 | Esri Portal for ArcGIS | Server-Side Request Forgery (SSRF) | 11.4 and prior | https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2025-update-2-patch |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-3755 | 9,1 | Mitsubishi Electric Corporation MELSEC iQ-F Series CPU | Improper Validation of Specified Index, Position, or Offset in Input | | https://jvn.jp/vu/JVNVU94070048/ https://www.mitsubishielectric.com/psirt/vulnerability/pdf/2025-003_en.pdf |
| https://nvd.nist.gov/vuln/detail/CVE-2025-47933 | 9,0 | Argo CD | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | Prior to versions 2.13.8, 2.14.13, and 3.0.4 | https://github.com/argoproj/argo-cd/commit/a5b4041a79c54bc7b3d090805d070bcdb9a9e4d1 https://github.com/argoproj/argo-cd/security/advisories/GHSA-2hj5-g64g-fp6p |
| https://nvd.nist.gov/vuln/detail/CVE-2025-48734 | 8,8 | Apache Commons | Improper Access Control | version 1.9.2 | http://www.openwall.com/lists/oss-security/2025/05/28/6 https://lists.apache.org/thread/s0hb3jkfj5f3ryx6c57zqtfohb0of1g9 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-5063 | 8,8 | Google Chrome | Use After Free | Google Chrome prior to 137.0.7151.55 | https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_27.html https://issues.chromium.org/issues/411573532 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-5215 | 8,8 | D-Link | Improper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DCS-5020L 1.01_B2 | https://github.com/xiaobor123/vul-dlink-dcs5020l https://github.com/xiaobor123/vul-dlink-dcs5020l https://github.com/xiaobor123/vul-dlink-dcs5020l#poc https://vuldb.com/?ctiid.310311 https://vuldb.com/?id.310311 https://vuldb.com/?submit.582935 https://www.dlink.com/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-5228 | 8,8 | D-Link | Improper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DI-8100 up to 20250523 | https://github.com/xubeining/Cve_report/blob/main/The%20D-Link%20DI-8100%20contains%20a%20binary%20vulnerability.md https://vuldb.com/?ctiid.310326 https://vuldb.com/?id.310326 https://vuldb.com/?submit.583430 https://www.dlink.com/ |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-5280 | 8,8 | Google Chrome | Out-of-bounds Write | V8 in Google Chrome prior to 137.0.7151.55 | https://chromereleases.google-blog.com/2025/05/stable-channel-update-for-desk-top_27.html https://issues.chromium.org/issues/417169470 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-51392 | 8,8 | OpenKnowledgeMaps Headstart | Improper Input Validation | v7 | https://github.com/OpenKnowledgeMaps/Headstart https://github.com/manisashank/CVE-Publish/blob/main/CVE-2024-51392.md |
| https://nvd.nist.gov/vuln/detail/CVE-2025-48383 | 8,2 | Django | Transmission of Private Resources into a New Sphere ('Resource Leak') | Django-Select2 is a Django integration for Se-lect2. Prior to version 8.4.1 | https://github.com/codingjoe/django-select2/commit/e5f41e6edba004d35f94915ff5e2559f44853412 https://github.com/codingjoe/django-select2/security/advisories/GHSA-wjrh-hj83-3wh7 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-25251 | 7,8 | FortiClient | Incorrect Authorization | FortiClient Mac 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 | https://fortiguard.fortinet.com/psirt/FG-IR-25-016 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-5270 | 7,5 | Firefox | Cleartext Transmission of Sensitive Information | Firefox < 139 | https://bugzilla.mozilla.org/show_bug.cgi?id=1910298 Permissions Required https://www.mozilla.org/security/adviso-ries/mfsa2025-42/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-5334 | 7,5 | Remote Desktop Manager Windows | Exposure of Sensitive Information to an Un-authorized Actor | 2025.1.34.0 and earlier | https://devolutions.net/security/advisories/DEVO-2025-0009 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-4134 | 7,3 | Avast Business Antivirus | Files or Directories Acces-sible to External Parties | Avast Business Antivirus for Linux 4.5 | https://www.gendigital.com/us/en/contact-us/secu-rity-advisories/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-48797 | 7,3 | GIMP | Heap-based Buffer Overflow | | https://access.redhat.com/security/cve/CVE-2025-48797 https://bugzilla.redhat.com/show_bug.cgi?id=2368558 |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-5221 | 7,3 | FreeFloat FTP Server | Improper Restriction of Operations within the Bounds of a Memory Buffer | FreeFloat FTP Server 1.0.0 | https://fitoxs.com/exploit/exploit-62e89ab8b510813fd7e0a3a5fbc6e6b7f7e3ec7dd7c8f6244c82cf82dc11d51c.txt https://vuldb.com/?ctiid.310317 https://vuldb.com/?id.310317 https://vuldb.com/?submit.582971 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-5272 | 7,3 | Firefox 138 and Thunderbird 138 | Out-of-bounds Write | Firefox 138 and Thunderbird 138 | https://bugzilla.mozilla.org/buglist.cgi?bug_id=1726254%2C1742738%2C1960121 Broken Link https://www.mozilla.org/security/advisories/mfsa2025-42/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-5295 | 7,3 | FreeFloat FTP Server | Improper Restriction of Operations within the Bounds of a Memory Buffer | FreeFloat FTP Server 1.0.0 | https://fitoxs.com/exploit/exploit-4f6236b59b5119d64718e994b0f3d63a755e7cb5a496e3846b92dfb960f1a80a.txt https://vuldb.com/?ctiid.310420 https://vuldb.com/?id.310420 https://vuldb.com/?submit.582988 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-45474 | 7,3 | maccms10 | Server-Side Request Forgery (SSRF) | v2025.1000.4047 | https://www.yuque.com/morysummer/vx41bz/ptnnp4eema601rvz |

## CISA/CERT-EU Alerts & Advisories

| Σύντομη περιγραφή / Τίτλος | Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες | URL |
|---|---|---|
| CISA Releases One Industrial Control Systems Advisory | ICSA-25-146-01 Johnson Controls iSTAR Configuration Utility (ICU) Tool | https://www.cisa.gov/news-events/alerts/2025/05/27/cisa-releases-one-industrial-control-systems-advisory |
| Johnson Controls iSTAR Configuration Utility (ICU) Tool | https://cwe.mitre.org/data/definitions/457.html | https://www.cisa.gov/news-events/ics-advisories/icsa-25-146-01 |
| New Guidance for SIEM and SOAR Implementation | | https://www.cisa.gov/news-events/alerts/2025/05/27/new-guidance-siem-and-soar-implementation |
| CISA Publishes SIEM & SOAR Implementation Guide Exclusively for Cybersecurity Executives | | https://cybersecuritynews.com/cisa-siem-soar-implementation-guide/ |

## News

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Regulatory Compliance – Navigating Cybersecurity Laws | https://cybersecuritynews.com/regulatory-compliance-cybersecurity/ |
| Cybersecurity Skills Gap – Training the Next Generation | https://cybersecuritynews.com/cybersecurity-skills-gap/ |
| Velvet Chollima APT Hackers Attacking Government Officials With Weaponized PDF | https://cybersecuritynews.com/velvet-chollima-apt-hackers-attacking-government-officials/ |
| Security Trends Analysis – Emerging Risks for 2025 | https://cybersecuritynews.com/security-trends/ |
| Building a Cyber-Resilient Organization in 2025 | https://cybersecuritynews.com/cyber-resilient-organization/ |
| The Future of Cybersecurity – Trends Shaping the Industry | https://cybersecuritynews.com/future-of-cybersecurity/ |
| Incident Response Planning – Preparing for Data Breaches | https://cybersecuritynews.com/incident-response-planning/ |

## Breaches / Compromised / Hacked

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| 93+ Billion Stolen Users' Cookies Flooded by Hackers on the Dark Web | https://cybersecuritynews.com/93-billion-stolen-users-cookies/ |
| Hackers Allegedly Claim AT&T Data Leak – 31M Records Exposed | https://cybersecuritynews.com/hackers-allegedly-claim-att-data-leak/ |
| APT36 & Sidecopy Hackers Attacks India's Critical Infrastructure To Deploy Malware | https://cybersecuritynews.com/apt36-sidecopy-hackers-attacks-indias-critical-infrastructure/ |
| Data broker giant LexisNexis says breach exposed personal information of over 364,000 people | https://techcrunch.com/2025/05/28/data-broker-giant-lexisnexis-says-breach-exposed-personal-information-of-over-364000-people/?&web_view=true |
| More than $12 million stolen from crypto platform Cork Protocol | https://therecord.media/cork-protocol-defi-12million-crypto-theft?&web_view=true |
| 1.6 Million Customer Emails Exposed in Etsy and TikTok Shop Data Leak | https://dailysecurityreview.com/security-spotlight/1-6-million-customer-emails-exposed-in-etsy-and-tiktok-shop-data-leak/ |
| MATLAB With Over 5 Million Customers Suffers Ransomware Attack | https://cybersecuritynews.com/matlab-ransomware-attack/ |

## Vulnerabilities / Flaws / Zero-day

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Critical Firefox 0-Interaction libvpx Vulnerability Let Attackers Execute Arbitrary Code | https://cybersecuritynews.com/firefox-0-interaction-libvpx-vulnerability/ |
| #Infosec2025: Over 90% of Top Email Domains Vulnerable to Spoofing Attacks | https://www.infosecurity-magazine.com/news/infosec2025-email-domains-spoofing/ |
| Apache Tomcat CGI Servlet Vulnerability Allows Security Constraint Bypass | https://cybersecuritynews.com/apache-tomcat-cgi-servlet-vulnerability/ |

## Patches / Updates / Fixes

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Chrome Security Update – High-Severity Vulnerabilities Lead to Code Execution | https://cybersecuritynews.com/chrome-security-update-code-execution/ |
| Mozilla releases Firefox 139.0.1 update to fix artifacts on Nvidia GPUs | https://www.bleepingcomputer.com/news/software/mozilla-releases-firefox-13901-update-to-fix-artifacts-on-nvidia-gpus/ |

## Potential threats / Threat intelligence

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Silver RAT Malware With New Anti-virus Bypass Techniques Executes Malicious Activities | https://cybersecuritynews.com/silver-rat-malware-with-new-anti-virus-bypass-techniques/ |
| New Botnet Hijacks 9,000 ASUS Routers & Enables SSH Access by Injecting Public Key | https://cybersecuritynews.com/new-botnet-hijacks-9000-asus-routers/ |
| Hackers Actively Exploiting Cloudflare Tunnels for Stealthy Attacks | https://cybersecuritynews.com/hackers-actively-exploiting-cloudflare-tunnels/ |
| Microsoft OneDrive File Picker Vulnerability Exposes Users' Entire Cloud Storage to Websites | https://cybersecuritynews.com/onedrive-file-picker-vulnerability/ |
| WordPress TI WooCommerce Wishlist Plugin Vulnerability Exposes 100,000+ Web-sites To Cyberattack | https://cybersecuritynews.com/wordpress-ti-woocommerce-wishlist-plugin-vulnerability/ |
| Hackers Mimic Popular Antivirus Site to Deliver VenomRAT & Steal Finance Data | https://cybersecuritynews.com/hackers-mimic-popular-antivirus-site/ |

## 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.

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

## 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/<br>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<br>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<br>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/ |