

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

**Date: 13/06/2025 - 17/06/2025**





Contents

[**Common Vulnerabilities and Exposures (CVEs)** 3](#_Toc201046982)

[**CISA/CERT-EU Alerts & Advisories** 12](#_Toc201046983)

[**News** 12](#_Toc201046984)

[**Breaches / Compromised / Hacked** 12](#_Toc201046985)

[**Vulnerabilities / Flaws / Zero-day** 13](#_Toc201046986)

[**Patches / Updates / Fixes** 13](#_Toc201046987)

[**Potential threats / Threat intelligence** 14](#_Toc201046988)

[**Guides / Tools** 14](#_Toc201046989)

[References 15](#_Toc201046990)

[Annex – Websites with vendor specific vulnerabilities 16](#_Toc201046991)

# **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-2025-6098> | **9,8** | UTT | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Improper Restriction of Operations within the Bounds of a Memory Buffer | UTT 进取 750W up to 5.0 | https://github.com/newym/cve/blob/main/utt1.md https://github.com/newym/cve/blob/main/utt1.md#poc https://vuldb.com/?ctiid.312567 https://vuldb.com/?id.312567 https://vuldb.com/?submit.589437 |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6121> | **9,8** | D-Link | Stack-based Buffer OverflowImproper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DIR-632 FW103B08 | https://github.com/xiaobor123/vul-finds/tree/main/vul-find-dir632-dlink-get\_pure\_content https://github.com/xiaobor123/vul-finds/tree/main/vul-find-dir632-dlink-get\_pure\_content#poc https://vuldb.com/?ctiid.312590 https://vuldb.com/?id.312590 https://vuldb.com/?submit.592574 https://www.dlink.com/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6090> | **8,8** | H3C | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | H3C GR-5400AX V100R009L50 | https://github.com/CH13hh/cve/blob/main/new/5.md https://vuldb.com/?ctiid.312557 https://vuldb.com/?id.312557 https://vuldb.com/?submit.587999 |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6104> | **8,8** | Wifi-soft | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')Improper Neutralization of Special Elements used in a Command ('Command Injection') | Wifi-soft UniBox Controller up to 20250506 | https://github.com/h0e4a0r1t/h0e4a0r1t.github.io/blob/master/2025/1/Command%20Injection%20Vulnerability%20in%20Wifi-soft%20UniBox%20controller-billing-pms\_check.pdf https://vuldb.com/?ctiid.312573 https://vuldb.com/?id.312573 https://vuldb.com/?submit.590747 |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6110> | **8,8** | Tenda | Improper Restriction of Operations within the Bounds of a Memory BufferStack-based Buffer Overflow | Tenda FH1201 1.2.0.14(408) | https://lavender-bicycle-a5a.notion.site/Tenda-FH1201-fromSafeUrlFilter-20b53a41781f80bc8687e3887f536120?source=copy\_link https://vuldb.com/?ctiid.312579 https://vuldb.com/?id.312579 https://vuldb.com/?submit.592473 https://vuldb.com/?submit.592475 https://www.tenda.com.cn/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6111> | **8,8** | Tenda | Improper Restriction of Operations within the Bounds of a Memory BufferStack-based Buffer Overflow | Tenda FH1205 2.0.0.7(775) | https://lavender-bicycle-a5a.notion.site/Tenda-FH1205-fromVirtualSer-20b53a41781f809180a7d46f12f0417f?source=copy\_link https://vuldb.com/?ctiid.312580 https://vuldb.com/?id.312580 https://vuldb.com/?submit.592471 https://www.tenda.com.cn/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6112> | **8,8** | Tenda | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Improper Restriction of Operations within the Bounds of a Memory Buffer | Tenda FH1205 2.0.0.7 | https://lavender-bicycle-a5a.notion.site/Tenda-FH1205-fromadvsetlanip-20b53a41781f80bf850ff39f88ad7f2b?source=copy\_link https://vuldb.com/?ctiid.312581 https://vuldb.com/?id.312581 https://vuldb.com/?submit.592472 https://www.tenda.com.cn/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6113> | **8,8** | Tenda | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Improper Restriction of Operations within the Bounds of a Memory Buffer | Tenda FH1203 2.0.1.6 | https://lavender-bicycle-a5a.notion.site/Tenda-FH1203-fromadvsetlanip-20b53a41781f8070bc65ffadd1ed6bf1?source=copy\_link https://vuldb.com/?ctiid.312582 https://vuldb.com/?id.312582 https://vuldb.com/?submit.592478 https://www.tenda.com.cn/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6114> | **8,8** | D-Link | Stack-based Buffer OverflowImproper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DIR-619L 2.06B01 | https://github.com/wudipjq/my\_vuln/blob/main/D-Link6/vuln\_60/60.md https://github.com/wudipjq/my\_vuln/blob/main/D-Link6/vuln\_60/60.md#poc https://vuldb.com/?ctiid.312583 https://vuldb.com/?id.312583 https://vuldb.com/?submit.592568 https://www.dlink.com/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6115> | **8,8** | D-Link | Stack-based Buffer OverflowImproper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DIR-619L 2.06B01 | https://github.com/wudipjq/my\_vuln/blob/main/D-Link6/vuln\_62/62.md https://github.com/wudipjq/my\_vuln/blob/main/D-Link6/vuln\_62/62.md#poc https://vuldb.com/?ctiid.312584 https://vuldb.com/?id.312584 https://vuldb.com/?submit.592570 https://www.dlink.com/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6128> | **8,8** | TOTOLINK | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Improper Restriction of Operations within the Bounds of a Memory Buffer | TOTOLINK EX1200T 4.1.2cu.5232\_B20210713 | https://github.com/byxs0x0/cve2/blob/main/8.md https://github.com/byxs0x0/cve2/blob/main/8.md#poc https://vuldb.com/?ctiid.312597 https://vuldb.com/?id.312597 https://vuldb.com/?submit.592694 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6129> | **8,8** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK EX1200T 4.1.2cu.5232\_B20210713 | https://github.com/byxs0x0/cve2/blob/main/9.md https://github.com/byxs0x0/cve2/blob/main/9.md#poc https://vuldb.com/?ctiid.312598 https://vuldb.com/?id.312598 https://vuldb.com/?submit.592695 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6137> | **8,8** | TOTOLINK | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK T10 4.1.8cu.5207 | https://candle-throne-f75.notion.site/TOTOLINK-T10-setWiFiScheduleCfg-20ddf0aa11858053a171f052787c202f https://vuldb.com/?ctiid.312606 https://vuldb.com/?id.312606 https://vuldb.com/?submit.592911 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6138> | **8,8** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK T10 4.1.8cu.5207 | https://candle-throne-f75.notion.site/TOTOLINK-T10-setWizardCfg-20ddf0aa1185808892f1dbbf63e6a153?pvs=73 https://vuldb.com/?ctiid.312607 https://vuldb.com/?id.312607 https://vuldb.com/?submit.592917 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6144> | **8,8** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK EX1200T 4.1.2cu.5232\_B20210713 | https://github.com/awindog/cve/blob/main/688/1.md https://github.com/awindog/cve/blob/main/688/1.md#poc https://vuldb.com/?ctiid.312619 https://vuldb.com/?id.312619 https://vuldb.com/?submit.593009 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6145> | **8,8** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK EX1200T 4.1.2cu.5232\_B20210713 | https://github.com/awindog/cve/blob/main/688/2.md https://github.com/awindog/cve/blob/main/688/2.md#poc https://vuldb.com/?ctiid.312620 https://vuldb.com/?id.312620 https://vuldb.com/?submit.593011 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6146> | **8,8** | TOTOLINK | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Improper Restriction of Operations within the Bounds of a Memory Buffer | TOTOLINK X15 1.0.0-B20230714.1105 | https://github.com/Lena-lyy/cve/blob/main/3.md https://github.com/Lena-lyy/cve/blob/main/3.md#poc https://vuldb.com/?ctiid.312621 https://vuldb.com/?id.312621 https://vuldb.com/?submit.593014 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6147> | **8,8** | TOTOLINK | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Improper Restriction of Operations within the Bounds of a Memory Buffer | TOTOLINK A702R 4.0.0-B20230721.1521 | https://github.com/Lena-lyy/cve/blob/main/4.md https://github.com/Lena-lyy/cve/blob/main/4.md#poc https://vuldb.com/?ctiid.312622 https://vuldb.com/?id.312622 https://vuldb.com/?submit.593015 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6148> | **8,8** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK A3002RU 3.0.0-B20230809.1615 | https://github.com/Lena-lyy/cve/blob/main/5.md https://github.com/Lena-lyy/cve/blob/main/5.md#poc https://vuldb.com/?ctiid.312623 https://vuldb.com/?id.312623 https://vuldb.com/?submit.593018 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6149> | **8,8** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK A3002R 4.0.0-B20230531.1404 | https://github.com/Lena-lyy/cve/blob/main/6.md https://github.com/Lena-lyy/cve/blob/main/6.md#poc https://vuldb.com/?ctiid.312624 https://vuldb.com/?id.312624 https://vuldb.com/?submit.593019 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6150> | **8,8** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK X15 1.0.0-B20230714.1105 | https://github.com/Lena-lyy/cve/blob/main/688/7.md https://github.com/Lena-lyy/cve/blob/main/688/7.md#poc https://vuldb.com/?ctiid.312625 https://vuldb.com/?id.312625 https://vuldb.com/?submit.593021 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6151> | **8,8** | TP-Link | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TP-Link TL-WR940N V4 | https://github.com/WhereisDoujo/CVE/issues/7 https://vuldb.com/?ctiid.312626 https://vuldb.com/?id.312626 https://vuldb.com/?submit.593031 https://www.tp-link.com/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6158> | **8,8** | D-Link | Stack-based Buffer OverflowImproper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DIR-665 1.00 | https://nvd.nist.gov/vuln/detail/CVE-2025-6158 |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-33108> | **8,5** | IBM | Execution with Unnecessary Privileges | IBM Backup, Recovery and Media Services for i 7.4 and 7.5 could | <https://www.ibm.com/support/pages/node/7236663> |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-24311> | **8,4** | Dell | Out-of-bounds Read | Dell ControlVault3 prior to 5.15.10.14 and Dell ControlVault3 Plus prior to 6.2.26.36 | <https://www.dell.com/support/kbdoc/en-us/000276106/dsa-2025-053> |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-1411> | **7,8** | IBM | Execution with Unnecessary Privileges | IBM Security Verify Directory Container 10.0.0.0 through 10.0.3.1 could | <https://www.ibm.com/support/pages/node/7236658> |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6130> | **7,4** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK EX1200T 4.1.2cu.5232\_B20210713 | https://github.com/byxs0x0/cve2/blob/main/10.md https://github.com/byxs0x0/cve2/blob/main/10.md#poc https://vuldb.com/?ctiid.312599 https://vuldb.com/?id.312599 https://vuldb.com/?submit.592696 https://www.totolink.net/ |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-6143> | **7,4** | TOTOLINK | Improper Restriction of Operations within the Bounds of a Memory BufferBuffer Copy without Checking Size of Input ('Classic Buffer Overflow') | TOTOLINK EX1200T 4.1.2cu.5232\_B20210713 | https://github.com/awindog/cve/blob/main/13.md https://vuldb.com/?ctiid.312618 https://vuldb.com/?id.312618 https://vuldb.com/?submit.593004 https://www.totolink.net/ |

# **CISA/CERT-EU Alerts & Advisories**

|  |  |  |
| --- | --- | --- |
| Σύντομη περιγραφή / Τίτλος | Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες | URL |
| CISA Adds Two Known Exploited Vulnerabilities to Catalog | * [CVE-2025-43200](https://www.cve.org/CVERecord?id=CVE-2025-43200) Apple Multiple Products Unspecified Vulnerability
* [CVE-2023-33538](https://www.cve.org/CVERecord?id=CVE-2023-33538) TP-Link Multiple Routers Command Injection Vulnerability
 | <https://www.cisa.gov/news-events/alerts/2025/06/16/cisa-adds-two-known-exploited-vulnerabilities-catalog>  |

# **News**

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
| NIST Released 19 Zero Trust Architecture Implementations Guide – What’s New | <https://cybersecuritynews.com/nist-zero-trust-architecture-guide/>  |
| Kali Linux 2025.2 Released: Smartwatch Wi-Fi Injection, Android Radio, and Hacking Tools | <https://cybersecuritynews.com/kali-linux-2025-2/>  |
| Gunra Ransomware Group Allegedly Leaks 40TB of Data from American Hospital | <https://cybersecuritynews.com/gunra-ransomware-group-leaks/>  |
| Microsoft Investigating Teams and Exchange Online Services Disruption Impacting Users | <https://cybersecuritynews.com/teams-and-exchange-online-services-disruption/>  |
| Washington Post Journalists’ Microsoft Accounts Hacked in Targeted Cyberattack | <https://cybersecuritynews.com/washington-post-journalists-microsoft-accounts-hacked/>  |
| Microsoft Outlook Users Face Crashes When Creating New Emails, Temp Fix Issued | <https://cybersecuritynews.com/microsoft-outlook-users-face-crashes/>  |
| Hackers Can Hide Images in Text Data and Embeds Directly into DNS TXT Records | <https://cybersecuritynews.com/hiding-images-in-dns-txt-records/>  |

# **Breaches / Compromised / Hacked**

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
| Zoomcar Hacked – 8.4 Million Users’ Sensitive Details Exposed | <https://cybersecuritynews.com/zoomcar-hacked/>  |

# **Vulnerabilities / Flaws / Zero-day**

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
| IBM Backup Services Vulnerability Let Attackers Escalate Privileges | <https://cybersecuritynews.com/ibm-backup-services-vulnerability/>  |
| Detecting Zero-Day Vulnerabilities in .NET Assemblies With Claude AI | <https://cybersecuritynews.com/zero-day-vulnerabilities-in-net-assemblies/>  |
| Acer Control Center Vulnerability Let Attackers Execute Malicious Code as a Privileged User | <https://cybersecuritynews.com/acer-control-center-vulnerability/>  |
| PoC Exploit Released for Windows Disk Cleanup Tool Elevation of Privilege Vulnerability | <https://cybersecuritynews.com/poc-exploit-released-for-windows-disk-cleanup-tool/>  |
| 46,000+ Grafana Instances Exposed to Malicious Account Takeover Attacks | <https://cybersecuritynews.com/grafana-account-takeover-attacks/>  |

# **Patches / Updates / Fixes**

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
|  |  |

# **Potential threats / Threat intelligence**

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
| GrayAlpha Hacker Group Weaponizes Browser Updates to Deploy PowerNet Loader and NetSupport RAT | <https://cybersecuritynews.com/grayalpha-hacker-group-weaponizes-browser-updates/>  |
| Anubis Ransomware With Wipe Mode That Permanently Erases File With No Recovery Option | <https://cybersecuritynews.com/anubis-ransomware-with-wipe-mode-that-permanently-erases-file/>  |
| Hundreds of WordPress Websites Hacked By VexTrio Viper Group to Run Massive TDS Services | <https://cybersecuritynews.com/hundreds-of-wordpress-websites-hacked-by-vextrio-viper-group/>  |
| AMOS macOS Stealer Hides in GitHub With Advanced Sophistication Methods | <https://cybersecuritynews.com/amos-macos-stealer-hides-in-github/>  |
| Threat Actors Attacking Cryptocurrency and Blockchain Developers with Weaponized npm and PyPI Packages | <https://cybersecuritynews.com/threat-actors-attacking-cryptocurrency-and-blockchain-developers/>  |
| Predator Mobile Spyware Remains Consistent with New Design Changes to Evade Detection | <https://cybersecuritynews.com/predator-mobile-spyware-remains-consistent/>  |
| Katz Stealer Enhances Credential Theft Capabilities with System Fingerprinting and Persistence Mechanisms | <https://cybersecuritynews.com/katz-stealer-enhances-credential-theft-capabilities/>  |
| Hackers Upload Weaponized Packages to PyPI Repositories to Steal AWS, CI/CD and macOS Data | <https://cybersecuritynews.com/hackers-upload-weaponized-packages-to-pypi-repositories/>  |
| 20+ Malicious Apps on Google Play Actively Attacking Users to Steal Login Credentials | <https://cybersecuritynews.com/malicious-apps-on-google-play/>  |
| North Korean APT Hackers Attacking Ukrainian Government Agencies to Steal Login Credentials | <https://cybersecuritynews.com/north-korean-apt-hackers-attacking-ukrainian-government-agencies/>  |
| Hackers Hijacked Discord Invite to Inject Malicious Links That Deliver AsyncRAT | <https://cybersecuritynews.com/hackers-hijacked-discord-invite-to-inject-malicious-links/>  |

# **Guides / Tools**

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
|  |  |

# 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/>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/>  |