POSTING DATE: 2025/12/17

[VULNERABILITY ALERT] CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2025/12/08-2025/12/14)

- Subject: [VULNERABILITY ALERT] CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2025/12/08-2025/12/14)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202512-00000007
  - [CVE-2022-37055] D-Link Routers Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
  - [Exploited by Ransomware: Unknown] D-Link routers contain a Buffer Overflow vulnerability, which has a high impact on confidentiality, integrity, and availability. Affected products may have reached End-of-Life (EoL) and/or End-of-Service (EoS) status, and users should stop using these products.
  - [CVE-2025-66644] Array Networks ArrayOS AG OS Command Injection Vulnerability (CVSS v3.1: 7.2)
  - [Exploited by Ransomware: Unknown] Array Networks ArrayOS AG contains an OS Command Injection vulnerability that may allow attackers to execute arbitrary commands.
  - [CVE-2025-6218] RARLAB WinRAR Path Traversal Vulnerability (CVSS v3.1: 7.8)
  - [Exploited by Ransomware: Unknown] RARLAB WinRAR contains a Path Traversal vulnerability, allowing an attacker to execute code as the current user.
  - [CVE-2025-62221] Microsoft Windows Use After Free Vulnerability (CVSS v3.1: 7.8)
  - [Exploited by Ransomware: Unknown] Microsoft Windows Cloud Files Mini Filter Driver contains a Use After Free vulnerability that may allow an authenticated attacker to elevate privileges locally.
  - [CVE-2025-58360] OSGeo GeoServer Improper Restriction of XML External Entity Reference Vulnerability (CVSS v3.1: 8.2)
  - [Exploited by Ransomware: Unknown] OSGeo GeoServer contains an Improper Restriction of XML External Entity Reference vulnerability. When the application receives XML input for the GetMap operation on the /geoserver/wms endpoint, it may allow an attacker to define external entities in the XML request.
  - [CVE-2018-4063] Sierra Wireless AirLink ALEOS Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 8.8)
  - [Exploited by Ransomware: Unknown] Sierra Wireless AirLink ALEOS contains an Unrestricted Upload of File with Dangerous Type vulnerability. An attacker can upload files via a specially crafted HTTP request, leading to the upload of executable code to the Web server, which can then be accessed over the network.
  - The attacker only needs to send an authenticated HTTP request to trigger this vulnerability. Affected products may have reached End-of-Life (EoL) and/or End-of-Service (EoS) status, and users should stop using these products.
  - [CVE-2025-14174] Google Chromium Out of Bounds Memory Access Vulnerability (CVSS v3.1: 8.8)

    - [Exploited by Ransomware: Unknown] Google Chromium's ANGLE component contains an Out of Bounds Memory Access vulnerability, which may allow a remote attacker to perform out-of-bounds memory access via a specially crafted HTML page. This vulnerability may affect multiple web browsers that use Chromium, including but not limited to Google Chrome, Microsoft Edge, and Opera.
- Affected Platforms:
    - [CVE-2022-37055] Please refer to the affected versions listed officially https://www.dlink.com/en/security-bulletin/
    - [CVE-2025-66644] ArrayOS AG versions prior to and including 9.4.5.8
    - [CVE-2025-6218] Please refer to the affected versions listed officially https://www.win-rar.com/singlenewsview.html
    - [CVE-2025-62221] Please refer to the affected versions listed officially https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62221
    - [CVE-2025-58360] Please refer to the affected versions listed officially https://github.com/geoserver/geoserver/security/advisories/GHSA-fjf5-xgmq-5525
    - [CVE-2018-4063] Sierra Wireless AirLink ES450 FW 4.9.3
    - [CVE-2025-14174] Please refer to the affected versions listed officially https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#december-11-2025
- Recommended Actions:
    - [CVE-2022-37055] Affected products may have reached End-of-Life (EoL) and/or End-of-Service (EoS) status, and users should stop using these products.
    - [CVE-2025-66644] Update the corresponding product to the following version (or later) ArrayOS AG 9.4.5.9
    - [CVE-2025-6218] The vendor has released a fix update for the vulnerability. Please update to the relevant version https://www.win-rar.com/singlenewsview.html
    - [CVE-2025-62221] The vendor has released a fix update for the vulnerability. Please update to the relevant version https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62221
    - [CVE-2025-58360] The vendor has released a fix update for the vulnerability. Please update to the relevant version https://github.com/geoserver/geoserver/security/advisories/GHSA-fjf5-xgmq-5525
    - [CVE-2018-4063] Affected products may have reached End-of-Life (EoL) and/or End-of-Service (EoS) status, and users should stop using these products.
    - [CVE-2025-14174] The vendor has released a fix update for the vulnerability. Please update to the relevant version https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#december-11-2025

Computer and Communication Center
Network Systems Division, Respectfully