JO-FinCERT – Security Advisory – 2023 – 46

1. ASUS urges customers to patch critical router vulnerabilities

ASUS has recently issued a firmware update for several router models, which includes cumulative security updates to address various vulnerabilities. Customers are strongly advised to update their devices immediately or restrict WAN (Wide Area Network) access until the devices are secured.

The newly released firmware includes fixes for nine security flaws, some of which are categorized as high or critical severity. Among the most severe vulnerabilities are CVE-2022-26376 and CVE-2018-1160.

CVE-2022-26376: A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. CVSS (9.8 / CRITICAL).

CVE-2018-1160: Netatalk before 3.1.12 is vulnerable to an out of bounds write in dsi_opensess.c. This is due to lack of bounds checking on attacker controlled data. A remote unauthenticated attacker can leverage this vulnerability to achieve arbitrary code execution. CVSS (9.8 /CRITICAL).

Reference: https://www.asus.com/content/asus-product-security-advisory/