مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in OpenWrt's ASU Feature

Tracking #:432316641

Date:17-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in OpenWrt's Attended Sysupgrade (ASU) feature, which could enable attackers to distribute and install malicious firmware packages on vulnerable devices.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2024-54143) with a CVSS score of 9.3 has been discovered in OpenWrt's Attended Sysupgrade (ASU) feature. This flaw could allow attackers to distribute malicious firmware packages, posing a significant threat to OpenWrt users.

The vulnerability stems from two main issues:

1. Command Injection: The imagebuilder service contains a flaw that allows attackers to inject arbitrary commands into the firmware build process
2. Truncated SHA-256 Hash: The request hashing mechanism truncates SHA-256 hashes to 12 characters, significantly reducing entropy and enabling attackers to generate collisions

These vulnerabilities combined allow attackers to:

- Inject malicious code into firmware images
- Sign compromised firmware with legitimate build keys
- Replace legitimate firmware builds with malicious ones in the artifact cache

No authentication is required to exploit these vulnerabilities, making them particularly dangerous. The flaw affects the OpenWrt sysupgrade server, potentially leading to the installation of malicious firmware during the attended firmware upgrade process.

Affected Versions:

- All versions of ASU prior to 920c8a1

Fixed Versions:

- ASU version 920c8a1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-54143