BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-70
Fecha de publicación: 18/12/2024
Tema: Vulnerabilidad Crítica en OpenWrt - CVE-2024-54143
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Versión ASU de Openwrt: 920c8a1

Descripción

Se ha identificado una vulnerabilidad crítica en la función Attended Sysupgrade (ASU) de OpenWrt, que podría permitir a atacantes distribuir firmware malicioso a través de imágenes comprometidas. Esta falla, clasificada como **CVE-2024-54143**, tiene una puntuación **CVSS de 9.3** y afecta directamente al servidor de actualización de sistema OpenWrt.

OpenWrt es un popular sistema operativo basado en Linux de código abierto para enrutadores, puertas de enlace residenciales y otros dispositivos integrados que enrutan el tráfico de red.

El problema de dicha vulnerabilidad radica en dos aspectos principales:

- Inyección de comandos en Imagebuilder

Los nombres de paquetes proporcionados por los usuarios son incorporados en los comandos make sin una validación adecuada. Esto permite que atacantes inyecten comandos arbitrarios durante el proceso de compilación, generando imágenes de firmware maliciosas firmadas con claves legítimas.

- Colisiones en hashes SHA-256 truncados

El mecanismo de hash de solicitud utiliza solo los primeros 12 caracteres del hash SHA-256, reduciendo significativamente la entropía. Esto facilita a los atacantes generar colisiones y reemplazar imágenes legítimas con versiones maliciosas, comprometiendo la integridad del firmware.

Estas fallas, explotadas en conjunto, podrían permitir a atacantes distribuir firmware comprometido mediante el servicio Attended Sysupgrade, afectando la confiabilidad y seguridad de las compilaciones entregadas.

No se necesita autenticación para explotar estas vulnerabilidades. Aunque la probabilidad de que existan imágenes comprometidas es baja, los usuarios quedan expuestos al riesgo de instalar firmware malicioso.

Solución

Las vulnerabilidades identificadas han sido solucionadas mediante las siguientes confirmaciones en el repositorio oficial de OpenWrt:

- commit deadda8097d4 ("build_request: seguridad: crítico: corregir la validación de entrada del usuario")
  https://github.com/openwrt/asu/commit/deadda8097

- commit d4c9e8b555ee ("util: seguridad: crítico: usar longitud de hash completa")
  https://github.com/openwrt/asu/commit/d4c9e8b555

Puede encontrar las actualización de su firmware en el siguiente enlace:
https://firmware-selector.openwrt.org/

Información adicional:

- https://lists.openwrt.org/pipermail/openwrt-announce/2024-December/000062.html
- https://thehackernews.com/2024/12/critical-openwrt-vulnerability-exposes.html
- https://flatt.tech/research/posts/compromising-openwrt-supply-chain-sha256-collision/

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com