BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-63
Fecha de publicación: 05/11/2024
Tema: Vulnerabilidad en el software Cisco Ultra-Reliable Wireless Backhaul (URWB)
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Los iguiente productos puede ser afectados solo sí tiene la versión del software afectado y tienen el modo URWB activado:

- Catalyst IW9165D Heavy Duty Access Points
- Catalyst IW9165E Rugged Access Points and Wireless Client
- Catalyst IW9167E Heavy Duty Access Points

La version del software Cisco Unified Industrial Wireless afectado son:

- 17.14 y anteriores
- 17.15

Descripción

Recientemente el equipo de Cisco ha publicado una vulnerabilidad de máxima gravedad de tipo Inyección de Comando (Command Injection) que afecta a los puntos de acceso Cisco Unified Wireless Radio Bands (UWRB) etiquetada como CVE-2024-20418 con un score CVSS de 10. Esta vulnerabilidad permitiría a un atacante remoto ejecutar comandos como root.

Esta vulnerabilidad de seguridad, se encontró en la interfaz de administración basada en web del software Unified Industrial Wireless de Cisco. Los actores de amenazas no autenticados pueden explotarla en ataques de inyección de comandos de baja complejidad que no requieren la interacción del usuario.

El equipo de Cisco informó que "Esta vulnerabilidad se debe a una validación incorrecta de la entrada a la interfaz de administración basada en la web. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes HTTP diseñadas a la interfaz de administración basada en la web de un sistema afectado"

Actualmente, no se reportan indicios de explotación activa de dicha vulnerabilidad.

Una de las condiciones, para la ejecución exitosa de la vulnerabilidad es que el modo URWB este activado, para verificarlo, el administrador puede utilizar el siguiente comando CLI: "**show** mpls-config". Si el comando no esta disponible entonces el dispositivo no tiene el modo URWB activado y el dispositivo no esta afectado por la vulnerabilidad.

Solución

Los clientes de Cisco pueden realizar la actualización gratuitamente de sus dipositivos a la versión segura 17.15.1 de acuerdo a los terminos de seguridad y convensiones de la misma.

Cisco Unified Industrial Wireless Software Release	Primera Release corregido
17.14 y anteriores	Migrar a una version corregida.
17.15	17.15.1

Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs
- https://www.bleepingcomputer.com/news/security/cisco-bug-lets-hackers-run-commands-as-root-on-uwrb-access-points/

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com