Nro. Alerta:	AL-2024-030	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	14-nov-2024	**Vulnerabilidad crítica en puntos de acceso cisco habilitado URWB**	Pág.: **1** of **3**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Ejecución remota de código

Nivel de riesgo: Alto

II. ALERTA

La vulnerabilidad CVE-2024-20418 es un fallo crítico en el software de Cisco Unified Industrial Wireless que afecta a los puntos de acceso que tienen habilitado el modo de Ultra-Reliable Wireless Backhaul (URWB).

Con un puntaje CVSS de 10.0 (máximo), esta vulnerabilidad permite a atacantes remotos y no autenticados ejecutar comandos con privilegios de root en el sistema operativo de los dispositivos afectados.

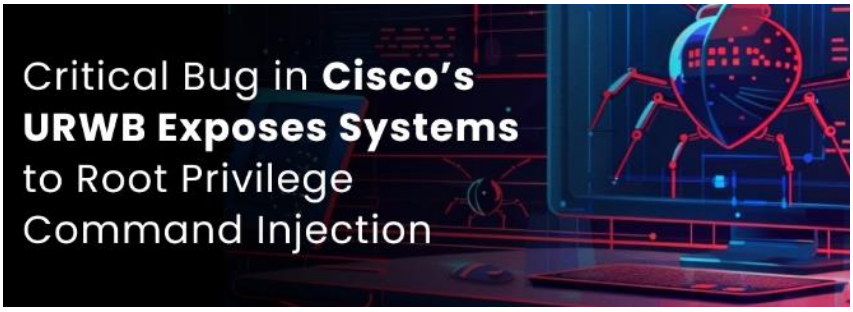

Figura 1: Imagen referencial vulnerabilidad CVE-2024-20418

III. INTRODUCCIÓN

Cisco anunció el pasado 6 de noviembre, parches para docenas de vulnerabilidades en sus productos empresariales, incluyendo una falla de gravedad crítica en el software Unified Industrial Wireless que afecta a los puntos de acceso que tengan habilitado el modo operativo de Cisco Ultra-Reliable Wireless Backhaul (URWB).

El error crítico, identificado como CVE-2024-20418, permite a un atacante remoto no autenticado inyectar comandos en el sistema operativo subyacente, con privilegios de root. El problema existe porque la interfaz de gestión basada en web de la solución de red industrial (*Unified Industrial Wireless*) no valida correctamente la entrada, lo que permite que un atacante envíe solicitudes HTTP diseñadas. Esta vulnerabilidad de seguridad afecta siempre y cuando se tenga habilitado el modo operativo URWB en los siguientes productos:

- Puntos de acceso (Access Point) de servicio pesado Catalyst IW9165D
- Puntos de acceso (Access Point) robustos y clientes inalámbricos Catalyst IW9165E
- Puntos de acceso (Access Point) de servicio pesado Catalyst IW9167E

Para conocer si el modo operativo URWB está habilitado en los productos vulnerables, se utiliza el comando CLI *"show mpls-config".* Si el comando no está disponible, URWB está deshabilitado y el dispositivo no se verá afectado por esta vulnerabilidad. Hasta la fecha no se ha reportado explotación activa de esta vulnerabilidad en entornos reales.

IV. IMPACTO:

Si la explotación es exitosa con el envío de solicitudes HTTP diseñadas, el atacante puede obtener control total sobre el sistema afectado, lo cual supone un riesgo significativo en entornos industriales donde se emplean estos dispositivos para comunicaciones seguras y confiables

V. RECOMENDACIONES:

Cisco ha lanzado un parche en la versión **17.15.1** del software Cisco Unified Industrial Wireless para mitigar esta vulnerabilidad y recomienda que los usuarios que tengan versiones anteriores actualicen de inmediato; es decir que los usuarios que utilizan desde la versión 17.14 o anterior migren a la versión corregida.

VI. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VII. REFERENCIAS:

- https://www.securityweek.com/cisco-patches-critical-vulnerability-in-industrial-networking-solution/
- 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/
- https://www.fortiguard.com/threat-signal-report/5574/cisco-urwb-access-point-command-injection-vulnerability-cve-2024-20418
- https://thehackernews.com/2024/11/cisco-releases-patch-for-critical-urwb.html