BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-38
Fecha de publicación: 9/05/2025
Tema: Vulnerablidad máxima en Cisco IOS XE
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Los siguientes productos se ven afectados si tienen una versión vulnerable en ejecución y tienen activada la función de descarga de imágenes de AP fuera de banda:

- Controladores inalámbricos Catalyst 9800-CL para la nube
- Controlador inalámbrico integrado Catalyst 9800 para conmutadores de las series Catalyst 9300, 9400 y 9500
- Controladores inalámbricos de la serie Catalyst 9800
- Controlador inalámbrico integrado en puntos de acceso Catalyst

Descripción

Se ha publicado una vulnerabilidad de seguridad de máxima gravedad en su controlador inalámbrico IOS XE que podría permitir que un atacante remoto no autenticado cargue archivos arbitrarios en un sistema susceptible. La vulnerabilidad es identificada como CVE-2025-20188 con un score CVSSv3 10.

Esta vulnerabilidad se debe a la presencia de un token web JSON (JWT) codificado en un sistema afectado. Un atacante podría explotar esta vulnerabilidad enviando solicitudes HTTPS manipuladas a la interfaz de descarga de imágenes del punto de acceso. Una explotación exitosa podría permitirle cargar archivos, recorrer rutas y ejecutar comandos arbitrarios con privilegios de root.

Dicho esto, para que la explotación sea exitosa, la función de descarga de imágenes de AP fuera de banda debe estar habilitada en el dispositivo. Está deshabilitada por defecto.

Determinar la configuración del dispositivo

Para determinar si un dispositivo está configurado con la función de descarga de imágenes de AP fuera de banda habilitada, utilice el comando `show running-config | include ap upgrade`. Si el comando devuelve `ap upgrade method https`, como se muestra en el

siguiente ejemplo, la función está habilitada y el dispositivo se ve afectado por esta vulnerabilidad:

```
wlc# show running-config | include ap upgrade
ap upgrade method https
wlc#
```

Mitigación

Como medida de mitigación temporal, los administradores pueden deshabilitar la función de descarga de imágenes de AP fuera de banda hasta que se pueda realizar una actualización.

Solución

El proveedor ha publicado parches de seguridad que mitigan diche vulnerabilidad, puede contactar al equipo de Soporte de Cisco para instrucciones de como mitigarlo o utilizar el siguiente enlace:
https://www.cisco.com/c/en/us/support/index.html

También puede dirigirse al enlace del boletín oficial de seguridad del Cisco para más información al respecto:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC

Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC
- https://thehackernews.com/2025/05/cisco-patches-cve-2025-20188-100-cvss.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-20188

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com