BOLETÍN DE ALERTA

Boletín Nro.: 2023-49
Fecha de publicación: 17/10/2023
Tema: Vulnerabilidad Crítica para CISCO IOS XE

Productos afectados:

- Cisco IOS XE Software, versión 17.6.x
- Cisco IOS XE Software, versión 17.7.x
- Cisco IOS XE Software, versión 17.8.x
- Cisco IOS XE Software, versión 17.9.x
- Cisco IOS XE Software, versión 18.0.x
- Cisco IOS XE Software, versión 18.1.x
- Cisco IOS XE Software, versión 18.2.x

Descripción:

El Fabricante Cisco ha publicado un aviso de seguridad para una vulnerabilidad de escalada de privilegios en la interfaz de usuario web (UI) de Cisco IOS XE Software, denominada CVE-2023-20198. Esta vulnerabilidad permite a un actor malicioso no autenticado, crear una cuenta con privilegios de nivel 15 en un dispositivo afectado.

La vulnerabilidad se debe a un error en la forma en que la *UI* verifica la autenticación de los usuarios. Un actor malicioso podría aprovecharse de esta falla enviando un paquete de solicitud de autenticación malformado que la *UI* no puede validar correctamente. Esto permite al atacante crear una cuenta con privilegios de nivel 15 sin tener que proporcionar ninguna información de autenticación válida.

Impacto:

Un actor malicioso podría aprovechar esta vulnerabilidad, para tomar el control total del dispositivo afectado por la vulnerabilidad. Esto permitiría a un actor malicioso acceder a datos confidenciales, realizar cambios en la configuración del dispositivo o incluso interrumpir el servicio.

Solución:

Cisco ha publicado una actualización de software para corregir esta vulnerabilidad. Los usuarios de Cisco IOS XE Software deben aplicar esta actualización lo antes posible para mitigar el riesgo de explotación de esta vulnerabilidad.

Recomendaciones:

Para mitigar el riesgo de explotación de esta vulnerabilidad, Cisco recomienda:

- Instalar la actualización de software de Cisco lo antes posible
- Desactivar la interfaz de usuario web si no la necesita

Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
- https://nvd.nist.gov/vuln/detail/CVE-2023-20198