BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-42
Fecha de publicación: 26/09/2024
Tema: CVE-2024-7479 Verificacion Inapropiada de la Firma Criptografica
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Versiones de TeamViewer anteriores a 15.58.4

Descripción

Se ha identificado una vulnerabilidad de alta severidad en TeamViewer Remote para Windows que podría permitir a un atacante con acceso físico al dispositivo obtener permisos de administrador.

La vulnerabilidad se origina debido a una falla en la validación de la firma criptográfica en la instalación de controladores en sistemas Windows. Este proceso es clave para garantizar que los controladores sean auténticos y no hayan sido alterados. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local elevar privilegios e instalar controladores de manera no autorizada.

Solución

Se recomienda a todos los usuarios actualizar a la versión 15.58.4 o superior de TeamViewer Remote para mitigar esta vulnerabilidad.

- Descargue la última versión disponible de TeamViewer Remote desde el sitio web oficial.
- Asegúrese de contar con un plan para actuar rápidamente en caso de brechas de seguridad o ciberataques.

La actualización de seguridad corrige esta vulnerabilidad, evitando que pueda ser explotada por ciberdelincuentes con acceso local al sistema. Mantener su software actualizado es clave para prevenir posibles ataques.

Información adicional:

- https://www.incibe.es/empresas/avisos/actualizacion-en-teamviewer-para-evitar-una-verificacion-incorrecta-de-la
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-7479
- https://nvd.nist.gov/vuln/detail/CVE-2024-7479

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com