Alerta de seguridad informática	9VSA20-00134-02
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de abril de 2020
Última revisión	22 de abril de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por TeamViewer referente a vulnerabilidad que afecta a su sistema de encriptación de credenciales. El presente informe incluye la respectiva medida de mitigación.

VULNERABILIDAD

CVE-2019-18988

CVE-2019-18998

Impacto

Es posible evadir el control de acceso de inicio de sesión remoto debido a que la aplicación utiliza la misma llave AES en las instalaciones de diferentes clientes para cifrar el proxy almacenado y la clave de opciones. Un atacante que tenga acceso al dispositivo podría reutilizar esta llave para descifrar las credenciales que almacena la aplicación.

Productos Afectados

TeamViewer versiones 8.x, 9.x, 10.x, 11.x, 12.x, 13.x y 14.x.

Mitigación

Actualizar a la versión 14.7.39531 de TeamViewer.

Enlaces

https://community.teamviewer.com/t5/Change-Logs/Windows-v14-7-39531-Full-Change-Log/td-p/90813
https://community.teamviewer.com/t5/Anuncios-ES/Más-especificaciones-sobre-CVE-2019-18988/td-p/82271
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18998