Alerta de seguridad informática	9VSA20-00228-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2020
Última revisión	27 de mayo 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 obtenida de OpenSSH referente a vulnerabilidad que a la aplicación de comunicaciones cifradas por red. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CWE-399

CWE-399

Esta vulnerabilidad permitiría a un atacante escribir archivos arbitrarios en el sistema de la víctima. Debido a la incorrecta administración del “scp(1)” al recibir archivos, un atacante remoto que controle el sistema de archivos podría diseñar un sistema que transfiera diferentes nombres de archivos y contenidos al diseño del sistema de archivos del usuario real.

Productos Afectados

OpenSSH desde la versión 5.0p1 hasta la 8.2p1.

Mitigación

Actualizar a la versión 8.3 de OpenSSH.

Enlaces

https://www.openssh.com/txt/release-8.3