Alerta de seguridad cibernética	9VSA20-00260-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de julio de 2020
Última revisión	03 de julio 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 múltiples fuentes referente a una vulnerabilidad que cliente de conexión remota PuTTY. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-14002

CVE-2020-14002

Si un servidor SSH aceptó una oferta de una llave pública, y luego rechazó la firma, PuTTY podría acceder a la memoria liberada, si es que la llave vino de un agente SSH.

Productos Afectados

PuTTY versiones 0.68, 0.69, 0.70, 0.71, 0.72 y 0.73.

Mitigación

Actualizar a la versión 0.74 de PuTTY.

Enlaces

https://lists.tartarus.org/pipermail/putty-announce/
https://www.chiark.greenend.org.uk/~sgtatham/putty/changes.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14002