Alerta de seguridad informática	9VSA-00062-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Octubre de 2019
Última revisión	08 de Octubre de 2019

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 diferentes fuentes referente a vulnerabilidades que afectan al aplicativo Putty.

Vulnerabilidad

CVE-2019-17067
CVE-2019-17068
CVE-2019-17069

Impacto

CVE-2019-17067

La vulnerabilidad permite que un usuario local altere la conexión de la aplicación. Esta vulnerabilidad existe debido a PuTTY cuando se instala en el sistema operativo Windows abre incorrectamente los sockets de escucha de reenvío de puertos. Un usuario local puede escuchar en el mismo puerto e interceptar todos los paquetes de conexión entrantes.

CVE-2019-17068

La vulnerabilidad permite que un atacante remoto evite ciertas restricciones de seguridad. Esta vulnerabilidad existe debido a un error con la implementación de protección "bracketed paste mode". Un atacante remoto puede afectar la sesión del usuario actual con un contenido malicioso del portapapeles y ejecutar comandos arbitrarios en un sistema remoto con privilegios del usuario actual.

CVE-2019-17069

La vulnerabilidad permite que un atacante remoto realice un ataque de denegación de servicio (DoS). La vulnerabilidad existe debido a un error al procesar el mensaje SSH1_MSG_DISCONNECT. Un atacante remoto puede engañar a la víctima para que se conecte a un servidor SSH-1 remoto, enviar un mensaje SSH1_MSG_DISCONNECT especialmente diseñado y bloquear el cliente PuTTY afectado.

Productos Afectados

Las siguientes versiones de Putty se encuentran afectadas por estas vulnerabilidades: 0.45, 0.46, 0.47, 0.48, 0.49, 0.50, 0.51, 0.52, 0.53, 0.54, 0.55, 0.56, 0.57, 0.58, 0.59, 0.60, 0.61, 0.62, 0.63, 0.64, 0.65, 0.66, 0.67, 0.68, 0.69, 0.70, 0.71, 0.72

Mitigación

Aplicar las actualizaciones publicadas por el fabricante, la versión 0.73 mitiga las vulnerabilidades.

Enlace

https://lists.tartarus.org/pipermail/putty-announce/2019/000029.html
https://lists.opensuse.org/opensuse-security-announce/2019-10/msg00021.html
https://www.cybersecurity-help.cz/vdb/SB2019100715

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.08 13:12:18 -03'00'