

Alerta de seguridad informática	9VSA-00068-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de octubre de 2019
Última revisión	16 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 afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Red Hat, referente a una vulnerabilidad que afecta a SUDO en la mayoría de las distribuciones de Linux, junto a sus respectivas actualizaciones para mitigar los riesgos.

Vulnerabilidades

- CVE-2019-14287

Impacto

Vulnerabilidad de tipo escalación de privilegios, la cual permite a un usuario con privilegios específicos, obtenidos a través de `/etc/sudoers`, escalar a nivel root.

Producto Afectado

Esta vulnerabilidad afecta a “sudo”. Todas las versiones anteriores a 1.8.27, incluida, son vulnerables. Para comprobar la versión, utilizar el comando “sudo -V”.

Mitigación

Actualizar a la última versión disponible de sudo (1.8.28)

Enlaces

<https://access.redhat.com/security/cve/cve-2019-14287>