

Alerta de Seguridad Informática (9VSA-00015-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 09 de Julio de 2019 | Última revisión 09 de Julio 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

VMware Security Response informó una vulnerabilidad parcial de denegación de servicio en ESXi. Los parches y soluciones están disponibles actualmente para remediar o solucionar esta vulnerabilidad

Vulnerabilidad

CVE-2019-5528

Impacto

Múltiples intentos fallidos de inicio de sesión en ESXi pueden hacer que el servicio hostd deje de responder, lo que resulta en una denegación parcial del servicio para la funcionalidad de administración. VMware ha evaluado la gravedad de este problema en el rango de gravedad Moderado con una puntuación base máxima de CVSSv3 de 5.3.

Productos afectados

ESXi 6.7

ESXi 6.5

Mitigación

Para la versión 6.5 se recomienda encarecidamente a los administradores de ESXi que apliquen el parche de seguridad **ESXi650-201907201-UG**


Hasta el cierre de la edición de este documento el parche para la versión 6.7 aún se encuentra pendiente, sin embargo existe una solución alternativa publicada en <https://kb.vmware.com/s/article/67920>

Enlaces

<https://www.vmware.com/es/security/advisories/VMSA-2019-0011.html>

Contactos

 <https://www.csirt.gob.cl>

 + (562) 24863850

 @CSIRTGOB

 <https://www.linkedin.com/company/csirt-gob>