Alerta de seguridad cibernética	9VSA-00097-002
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Diciembre de 2019
Última revisión	08 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 entregada por VMware referente a vulnerabilidad que afecta a ESXi y Horizon DaaS. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2019-5544

CVE-2019-5544

Debido a un error en memoria que afecta a los sistemas, un atacante con accedo a la red, y al puerto 427 podría sobrescribir la pila en memoria del servicio OpenSLP, resultando en la ejecución de código remoto y comprometiendo completamente al sistema.

Productos Afectados

VMware ESXi, versiones 6.0, 6.5 y 6.7.
VMware Horizon Daas, versiones 8.x.

Mitigación

Para ESXi versión 6.7, aplicar versión ESXi670-201912001.
Para ESXi versión 6.5, aplicar versión ESXi650-201912001.
Para ESXi versión 6.0, aplicar versión ESXi600-201912001.
Para Horizon DaaS versión 8.0, actualizar a la versión 9.0.0.0.

Enlaces

https://www.csirt.gob.cl/media/2019/12/9VSA-00097-001.pdf
https://www.vmware.com/security/advisories/VMSA-2019-0022.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5544