Alerta de seguridad informática	9VSA-00097-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de diciembre de 2019
Última revisión	6 de diciembre 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 información obtenida del sitio oficial de VMWare, referente a vulnerabilidades que afectan a sus productos ESXi y Horizon DaaS.

Vulnerabilidad

CVE-2019-5544

Impacto

OpenSLP, utilizado en ESXi y los dispositivos Horizon DaaS, tiene un problema de sobrescritura el la pila. VMware ha evaluado la gravedad de este problema para estar en el rango de gravedad crítica con una puntuación base máxima de CVSSv3 de 9.8.

Un actor malicioso con acceso de red al puerto 427 en un host ESXi o en cualquier dispositivo de administración Horizon DaaS puede sobrescribir la pila del servicio OpenSLP, lo que resulta en la ejecución remota de código.

Producto Afectado

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

Mitigación

Aplicar las actualizaciones a las versiones publicadas por el fabricante según corresponda. Hasta el momento de la publicación de este informe la actualización de seguridad para VMware Horizon aún se encuentra pendiente, se recomienda estar atentos a la liberación del parche para aplicarlo de forma inmediata.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2019-0022.html

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.06 18:14:04 -03'00'