Alerta de seguridad informática	9VSA20-00194-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de abril de 2020
Última revisión	29 de abril 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 VMware ESXi. El presente informe incluye la respectiva medida de mitigación.

VULNERABILIDAD

CVE-2020-3955

CVE-2020-3955

Debido a que el cliente Host ESXi no sanitiza correctamente los datos ingresados por el usuario al ver los atributos de las máquinas virtuales, un atacante remoto podría inyectar código HTML y script en el contexto del sitio vulnerable, permitiéndole cambiar la apariencia del sitio, robar información potencialmente sensible y engañar a una víctima para que descargue malware.

Productos Afectados

VMware ESXi 6.7 y 6.5.

Mitigación

Para la versión 6.7, actualizar a ESXi670-202004103-SG.
Para la versión 6.5, actualizar a ESXi650-201912104-SG.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0008.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3955