Alerta de seguridad informática	9VSA20-00220-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2020
Última revisión	20 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 obtenida de VMware referente a vulnerabilidad que afecta a Cloud Director. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-3956

CVE-2020-3956

Se ha subsanado una vulnerabilidad de tipo inyección de código, que puede ser explotada a través de HTML5 e interfaces de usuarios basadas en Flex, la interfaz de explorador de API y el acceso a la API, permitiendo a un atacante la ejecución de código arbitrario, comprometiendo completamente al sistema afectado.

Productos Afectados

vCloud Director versiones 9.1.x para Linux y 9.5.x, 9.7.x y 10.0.x para Linux y PhotonOS.

Mitigación

Para versiones 9.1.x, actualizar a la 9.1.0.4.
Para versiones 9.5.x, actualizar a la 9.5.0.6.
Para versiones 9.7.x, actualizar a la 9.7.0.5.
Para versiones 10.0.x, actualizar a la 10.0.0.2.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0010.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3956