

Alerta de seguridad informática	9VSA-00055-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de septiembre de 2019
Última revisión	25 de septiembre 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 la información entregada por VMware referente a una vulnerabilidad de escalamiento de privilegios en Harbor.

Vulnerabilidad

CVE-2019-16097

Impacto

Una vulnerabilidad en la API POST /api/users de Harbor puede permitir una escalada remota de privilegios. 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 usuario malicioso con acceso a la red de una API de POST /api/users de Harbor podría autorregistrar una nueva cuenta con privilegios administrativos. La explotación exitosa de este problema puede llevar a un compromiso completo del despliegue de Harbor.

Productos Afectados

- VMware Cloud Foundation (se ve afectado si el componente 'Harbor Registry' se encuentra desplegado)
- VMware Harbor Container Registry for PCF, versiones anteriores a 1.8.3
- VMware Harbor Container Registry for PCF, versiones anteriores a 1.7 .6

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

<https://www.vmware.com/security/advisories/VMSA-2019-0015.html>