Alerta de seguridad cibernética	9VSA22-00641-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	18 de mayo de 2022
Última revisión	18 de mayo de 2022

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre vulnerabilidades que afectan a productos de VMware.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2022-22972
CVE-2022-22973

Impacto

Vulnerabilidad crítica

CVE-2022-22972: Vulnerabilidad de evasión de autenticación que afecta a los usuarios de dominio local. VMware la considera crítica.

Productos afectados

VMware Workspace ONE Access (Access)
VMware Identity Manager (vIDM)
VMware vRealize Automation (vRA)
VMware Cloud Foundation
vRealize Suite Lifecycle Manager

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2022-0014.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22973