Alerta de seguridad cibernética	9VSA21-00449-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2021
Última revisión	27 de mayo de 2021

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 de Gobierno, comparte vulnerabilidades que afectan a VMware vCenter Server y VMware Cloud Foundation.

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

Vulnerabilidades

CVE-2021-21985
CVE-2021-21986

Impactos

CVE-2021-21985: Esta vulnerabilidad de ejecución remota de código en el vSphere Client (HTML5) tiene lugar debido a una falta de validación de la información ingresada en el plug-in Virtual SAN Health Check, que viene activado por defecto en vCenter Server. Esta vulnerabilidad es calificada como crítica por el proveedor.

CVE-2021-21986: Esta vulnerabilidad en el mecanismo de autenticación de varios plug ins de vSphere: Virtual SAN Health Check, Site Recovery, vSphere Lifecycle Manager, y VMware Cloud Director Availability. Esta vulnerabilidad es calificada como moderada por el proveedor.

Productos Afectados

vCenter Server 6.5 a 7.0.
Cloud Foundation (vCenter Server) 3.x, 4.x.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2021-0010.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21986

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.27 16:11:34 -04'00'