Alerta de seguridad cibernética	9VSA21-00495-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2021
Última revisión	22 de septiembre 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 del Gobierno de Chile, CSIRT de Gobierno, comparte información relacionada con vulnerabilidades divulgadas por VMware y que afectan a vCenter Server y Cloud Foundation.

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

Vulnerabilidades

CVE-2021-21991
CVE-2021-21992
CVE-2021-21993
CVE-2021-22005
CVE-2021-22006
CVE-2021-22007
CVE-2021-22008
CVE-2021-22009
CVE-2021-22010
CVE-2021-22011
CVE-2021-22012
CVE-2021-22013
CVE-2021-22014
CVE-2021-22015
CVE-2021-22016
CVE-2021-22017
CVE-2021-22018
CVE-2021-22019
CVE-2021-22020

Impactos

Críticas

CVE-2021-22005: Vulnerabilidad de carga arbitraria de archivos en el servicio Analytics de vCenter 6.7 y 7.0. Un actor malicioso con acceso de red al puerto 443 en vCenter Server puede explotar este problema para ejecutar código en vCenter Server cargando un archivo especialmente diseñado, sin importar la configuración de vCenter Server.

Riesgo alto

CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22006, CVE-2021-22007, CVE-2021-22008, CVE-2021-22009, CVE-2021-22010, CVE-2021-22011, CVE-2021-22014, CVE-2021-22015, CVE-2021-22017, CVE-2021-22018, CVE-2021-22019, CVE-2021-22020.

Productos Afectados

VMware vCenter Server
VMware Cloud Foundation

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2021-0020.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21993
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22020

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.22 18:02:22 -03'00'