

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Alerta de seguridad cibernética	9VSA22-00756-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	16 de diciembre de 2022
Última revisión	16 de diciembre 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 afectada a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información sobre varias vulnerabilidades que afectan a diversos productos de VMware.

Vulnerabilidades

CVE-2021-39144	CVE-2022-31693	CVE-2022-31700
CVE-2022-31678	CVE-2022-31696	CVE-2022-31701
CVE-2022-31685	CVE-2022-31697	CVE-2022-31705
CVE-2022-31686	CVE-2022-31698	CVE-2022-31707
CVE-2022-31687	CVE-2022-31699	CVE-2022-31708
CVE-2022-31688	CVE-2022-31702	
CVE-2022-31689	CVE-2022-31703	

Impacto

Vulnerabilidades de riesgo crítico

CVE-2021-39144: Vulnerabilidad de ejecución remota de código via XStream en VMware Cloud Foundation.

CVE-2022-31678: Vulnerabilidad XML External Entity (XXE) en VMware Cloud Foundation.

CVE-2022-31685: Vulnerabilidad de bypass de autenticación en VMware Workspace ONE Assist.

CVE-2022-31686: Vulnerabilidad de método de autenticación averiado en VMware Workspace ONE Assist.

CVE-2022-31687: Vulnerabilidad de control de acceso averiado en VMware Workspace ONE Assist.

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl

[@csirtgob](#)

<https://www.linkedin.com/company/csirt-gob>

CVE-2022-31688: Vulnerabilidad XSS en VMware Workspace ONE Assist.

CVE-2022-31689: Vulnerabilidad de fijación de sesión en VMware Workspace ONE Assist.

CVE-2022-31702: Vulnerabilidad de inyección de comandos en VMware vRealize Network Insight.

CVE-2022-31703: Vulnerabilidad de ataque transversal de directorio en VMware vRealize Network Insight (vRNI).

CVE-2022-31705: Vulnerabilidad de escritura fuera de límites en lotes en el controlador EHCI de VMware ESXi, Workstation y Fusion.

Productos afectados

VMware Cloud Foundation
VMware Workspace ONE Assist
VMware Tools for Windows
VMware ESXi and vCenter Server
VMware vRealize Network Insight (vRNI)
VMware Workspace ONE Access (Access)
VMware Identity Manager (vIDM)
VMware Cloud Foundation (Cloud Foundation)

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://www.vmware.com/security/advisories.html>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39144>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31678>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31685>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31686>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31687>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31688>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31689>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31693>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31696>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31697>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31698>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31699>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31702>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31703>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31700>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31701>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31705>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31707>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31708>