

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	9VSA22-00742-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	09 de noviembre de 2022
Última revisión	09 de noviembre 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 entregada por VMware sobre varias vulnerabilidades que afectan a Workspace ONE Assist.

Vulnerabilidades

CVE-2022-31685
CVE-2022-31686
CVE-2022-31687
CVE-2022-31688
CVE-2022-31689

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-31685: Vulnerabilidad de evasión de autenticación que podría ser abusada por un atacante con acceso de red a VMware Workspace ONE Assist para obtener acceso de administrador sin necesidad de autenticarse en la aplicación.

CVE-2022-31686: Vulnerabilidad de método de autenticación averiado.

CVE-2022-31687: Vulnerabilidad de control de acceso averiado.

CVE-2022-31688: Vulnerabilidad XSS derivada de una sanitización inapropiada de inputs, lo que podría ser explotada para inyectar código JavaScript arbitrario en la ventana del usuario objetivo.

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-2022-31689: Vulnerabilidad de fijación de sesión resultante de un manejo inapropiado de tokens de sesión. Un actor malicioso que obtenga un token de sesión válida puede autenticarse en la aplicación usando este token.

Productos afectados

VMware Workspace ONE Assist 21.x y 22.x. Las vulnerabilidades son parchadas en la versión 22.10.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://www.vmware.com/security/advisories/VMSA-2022-0028.html>

<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>