Alerta de seguridad cibernética	9VSA21-00475-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de julio de 2021
Última revisión	29 de julio 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 sobre vulnerabilidades que afectan al servidor de webmail de Zimbra.

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

Vulnerabilidades

CVE-2021-35208
CVE-2021-35209

Impactos

CVE-2021-35208: Vulnerabilidad existente debido a un error de cross-site scripting (XSS) que puede ser detonado con tan solo abrir un email malicioso que contenga una carga JavaScript.

CVE-2021-35209: Esta vulnerabilidad SSRF puede ser explotada por una cuenta autenticada perteneciente a la organización objetivo, sin importar qué rol o permiso tenga.

Productos Afectados

Zimbra 8.8.15, versiones anteriores al parche 18.
Zimbra 9.0, versiones anteriores al parche 16.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://wiki.zimbra.com/wiki/Security_Center
https://blog.sonarsource.com/zimbra-webmail-compromise-via-email
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35208
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35209

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.29 19:53:26 -04'00'