Alerta de seguridad cibernética	9VSA23-00873-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	28 de julio de 2023
Última revisión	28 de julio de 2023

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 CSIRT de Gobierno comparte información de una vulnerabilidad de día cero, ya explotada, que recientemente ha sido parchada por Zimbra para su Zimbra Collaboration Suite (ZCS).

Vulnerabilidades

CVE-2023-38750

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-38750: Vulnerabilidad de tipo cross-site scripting (XSS).

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Zimbra Collaboration Suite (ZCS) anteriores a ZCS 10.0.2.

Enlaces

https://wiki.zimbra.com/wiki/Security_Center#:~:text=for%20mitigation%20steps.-,ZCS%2010.0.2%20Released,-ZCS%2010.0.2%20was
https://info.zimbra.com/security-update-zimbra-collaboration-suite-version-8.8.15-important
https://www.cisa.gov/news-events/alerts/2023/07/27/cisa-adds-one-known-exploited-vulnerability-catalog
https://github.com/Zimbra/zm-web-client/pull/827
https://nvd.nist.gov/vuln/detail/CVE-2023-38750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38750

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.28 12:38:59 -04'00'