

Alerta de Seguridad Cibernética

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



Alerta de seguridad cibernética	9VSA23-00908-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	27 de septiembre de 2023
Última revisión	27 de septiembre 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 nueva vulnerabilidad crítica que afecta a la biblioteca de código abierto libwebp. Google puso a disposición un parche para esta vulnerabilidad cuando afecta a Google Chrome.

Vulnerabilidades

CVE-2023-5129

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-5129: Vulnerabilidad de desbordamiento de buffer en WebP que afecta a la biblioteca open-source libwebp y que había sido antes identificada por Google como un error de Chrome con el CVE CVE-2023-4863. Permite la escritura fuera de los límites de la memoria. Severidad 10/10 (Google). CVSS: 8.8.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Google Chrome anteriores a 116.0.5845.187.

Enlaces

<https://chromium.googlesource.com/webm/libwebp/+2af26267cdfcb63a88e5c74a85927a12d6ca1d76>

<https://chromium.googlesource.com/webm/libwebp/+902bc9190331343b2017211debcec8d2ab87e17a>

<https://www.openwall.com/lists/oss-security/2023/09/26/1>

<https://www.cve.org/CVERecord?id=CVE-2023-5129>

<https://nvd.nist.gov/vuln/detail/CVE-2023-5129>