

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	9VSA23-00876-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de agosto de 2023
Última revisión	2 de agosto 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 afectada a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de vulnerabilidades parchadas por Mozilla en Firefox 116, Firefox ESR 115.1 y Firefox ESR 102.14.

Vulnerabilidades

CVE-2023-4045
CVE-2023-4046
CVE-2023-4047
CVE-2023-4048
CVE-2023-4049
CVE-2023-4050
CVE-2023-4051
CVE-2023-4052
CVE-2023-4053
CVE-2023-4054
CVE-2023-4055
CVE-2023-4056
CVE-2023-4057
CVE-2023-4058

Impacto

Vulnerabilidades de riesgo alto

CVE-2023-4045: Vulnerabilidad en Offscreen Canvas que permite acceder a datos de imagen de otro sitio violando la política de same-origin.

CVE-2023-4046 En algunas circunstancias, puede resultar en compilación incorrecta y un bloqueo potencialmente explotable en el procesamiento de contenido.

CVE-2023-4047: Un error en el cálculo del delay de las notificaciones podría posibilitar a un atacante engañar al usuario para entregarle permisos.

CVE-2023-4048: Lectura fuera de los límites de la memoria que podría llevar a un bloqueo explotable.

CVE-2023-4049: Errores que podría resultar en vulnerabilidades potencialmente explotables de uso de memoria luego de ser liberada.

CVE-2023-4050: Vulnerabilidad que podría resultar en un bloqueo potencialmente explotable que podría llevar a un escape de sandbox.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Firefox, Firefox ESR.

Enlaces

<https://www.mozilla.org/en-US/security/advisories/mfsa2023-29/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4045>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4046>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4047>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4048>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4049>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4050>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4051>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4052>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4053>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4054>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4055>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4056>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4057>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4058>