

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	9VSA23-00889-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2023
Última revisión	31 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 sobre vulnerabilidades parchadas en Mozilla Firefox 117.

Vulnerabilidades

CVE-2023-4573
CVE-2023-4574
CVE-2023-4575
CVE-2023-4576
CVE-2023-4577

CVE-2023-4578
CVE-2023-4579
CVE-2023-4580
CVE-2023-4581
CVE-2023-4582

CVE-2023-4583
CVE-2023-4584
CVE-2023-4585

Impacto

Vulnerabilidades de riesgo alto

CVE-2023-4573: Vulnerabilidad de corrupción de memoria en IPC CanvasTranslator, podría llevar a causar un colapso potencialmente explotable.

CVE-2023-4574: Vulnerabilidad de corrupción de memoria en IPC ColorPickerShownCallback, podría llevar a causar un colapso potencialmente explotable.

CVE-2023-4575: Vulnerabilidad de corrupción de memoria en IPC FilePickerShownCallback, podría llevar a causar un colapso potencialmente explotable.

CVE-2023-4576: Vulnerabilidad de desborde de integrales en RecordedSourceSurfaceCreation, que podría llevar a una potencial brecha de datos sensibles y un escape de sandbox.

CVE-2023-4577: Vulnerabilidad de corrupción de memoria en JIT UpdateRedExpStatics, que podría llevar a un colapso potencialmente explotable.

CVE-2023-4584: Errores de memoria en Firefox 116, Firefox ESR 102.14, Firefox ESR 115.1, Thunderbird 102.14, y Thunderbird 115.1, que podría ser explotado para correr código arbitrario.

CVE-2023-4585: Errores de memoria en Firefox 116, Firefox ESR 102.14, Firefox ESR 115.1, Thunderbird 102.14, y Thunderbird 115.1, que podría ser explotado para correr código arbitrario.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Firefox 116, Firefox ESR 102.14, Firefox ESR 115.1, Thunderbird 102.14, y Thunderbird 115.1.

Enlaces

<https://www.mozilla.org/en-US/security/advisories/mfsa2023-34/>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4573>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4574>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4575>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4576>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4577>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4578>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4579>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4580>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4581>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4582>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4583>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4584>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4585>