Alerta de seguridad cibernética	9VSA23-00910-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	28 de septiembre de 2023
Última revisión	28 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 nuevas vulnerabilidades que han sido parchadas en Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3.

Vulnerabilidades

CVE-2023-5168
CVE-2023-5169
CVE-2023-5170
CVE-2023-5171
CVE-2023-5172
CVE-2023-5173
CVE-2023-5174
CVE-2023-5175
CVE-2023-5176

Impacto

Vulnerabilidades de riesgo alto

CVE-2023-5168: Vulnerabilidad que podría resultar en escritura fuera de los límites de la memoria y un crash potencialmente explotable en un proceso privilegiado. Solo afecta a Firefox en Windows.

CVE-2023-5169: Vulnerabilidad que podría resultar en escritura fuera de los límites de la memoria y un crash potencialmente explotable en un proceso privilegiado.

CVE-2023-5170: Vulnerabilidad que podría resultar en un memory leak en un proceso privilegiado. Este memory leak puede ser usado para efectuar un escape de sandbox.

CVE-2023-5171: Durante la compilación Ion, un Garbage Collection podría resultar en una condición use-after-free, permitiendo a un atacante escribir dos bytes NUL, provocando un cash explotable.

CVE-2023-5172: Vulnerabilidad que podría llevar a un crash potencialmente explotable.

CVE-2023-5176: Errores de seguridad de la memoria en Firefox 117, Firefox ESR 115.2 y Thunderbird 115.2 muestran evidencia de corrupción de memoria y la empresa supone que con suficiente esfuerzo podrían ser explotados para ejecutar código arbitrario.

Mitigación
Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados
Mozilla Firefox, Firefox ESR y Thunderbird.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2023-41/#CVE-2023-5172
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5168
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5169
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5170
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5171
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5172
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5173
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5174
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5175
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5176

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.28 13:56:23 -03'00'