Alerta de seguridad cibernética	9VSA23-00816-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2023
Última revisión	12 de abril 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 las vulnerabilidades parchadas por Mozilla en Firefox 112, Firefox for Android 112, Focus for Android 112 y Firefox ESR 102.10.

Vulnerabilidades

CVE-2023-29531	CVE-2023-29538	CVE-2023-29545
CVE-2023-29532	CVE-2023-29539	CVE-2023-29546
CVE-2023-29533	CVE-2023-29540	CVE-2023-29547
CVE-2023-29534	CVE-2023-29541	CVE-2023-29548
CVE-2023-29535	CVE-2023-29542	CVE-2023-29549
CVE-2023-29536	CVE-2023-29543	CVE-2023-29550
CVE-2023-29537	CVE-2023-29544	CVE-2023-29551

Impacto

Vulnerabilidades de riesgo alto

CVE-2023-29531: Vulnerabilidad de acceso de memoria fuera de límites en WebGL en macOS.
CVE-2023-29532: Vulnerabilidad de bypass de Mozilla Maintenance Service.
CVE-2023-29533: Vulnerabilidad que permite ocultar la notificación de la activación de la pantalla completa, lo que podría llevar a ataques de spoofing.
CVE-2023-29534: Vulnerabilidad que permite ocultar la notificación de la activación de la pantalla completa, lo que podría llevar a ataques de spoofing.
CVE-2023-29535: Vulnerabilidad en Garbage Collector compactor que puede llevar a corrupción de memoria y potencialmente un colapso del computador potencialmente explotable.
CVE-2023-29536: Vulnerabilidad que podría permitir a un atacante causar que el administrador de memoria libere incorrectamente elementos, resultando en corrupción de memoria o un colapso del computador potencialmente explotable.

CVE-2023-29537: Data races en el código de inicialización de fuentes, podría llevar a corrupción de memoria y la ejecución de código controlado por un atacante.

Productos afectados

Versiones anteriores a Firefox 112, Firefox for Android 112 y Focus for Android 112, y Firefox ESR anterior a Firefox ESR 102.10.

Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2023-13/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-14/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29531
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29532
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29533
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29534
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29535
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29536
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29537
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29538
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29539
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29540
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29541
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29542
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29543
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29544
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29545
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29546
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29547
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29548
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29549
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29550
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29551

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.04.12 11:55:08 -04'00'