Alerta de seguridad cibernética	9VSA22-00546-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2022
Última revisión	13 de enero de 2022

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 equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte nuevas vulnerabilidades en Mozilla Firefox.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2022-22746
CVE-2022-22743
CVE-2022-22742
CVE-2022-22744
CVE-2022-22741
CVE-2022-22740
CVE-2022-22738
CVE-2022-22737
CVE-2021-4140
CVE-2022-22749
CVE-2022-22750
CVE-2022-22748
CVE-2022-22745
CVE-2022-22744
CVE-2022-22747
CVE-2022-22736
CVE-2022-22739
CVE-2022-22751
CVE-2022-22752

Impactos

Vulnerabilidades de riesgo alto:

CVE-2022-22746: Vulnerabilidad que permite evadir la notificación de pantalla completa, lo que podría resultar en que un spoof de pantalla completa no sea detectado. Solo afecta a Firefox para Windows.

CVE-2022-22743: Vulnerabilidad que permite a un atacante controlar una pestaña y hacer que el navegador no deje el modo de pantalla completa.

CVE-2022-22742: Vulnerabilidad que permite que al insertar texto en el modo de edición, algunos caracteres puedan llevar a un acceso a memoria fuera de límites, causando una caída del sistema potencialmente explotable.

CVE-2022-22741: Vulnerabilidad que permite que al cambiar las dimensiones de un popup mientras se solicita acceso a la pantalla completa, el popup quede incapacitado de dejar el modo de pantalla completa.

CVE-2022-22740: Vulnerabilidad que permite que algunos objetos de solicitud de red (network request objects) se liberen demasiado pronto al liberar un identificador de solicitud de red (network request handle), lo que podría llevar a un error de uso de memoria después de ser liberada, y una caída del sistema potencialmente explotable.

CVE-2022-22738: Vulnerabilidad que podría llevar a un desbordamiento de heap buffer al aplicar un efecto de filtro CCS que puede haber accedido a memoria fuera de límites. Esto puede llevar a una caída potencialmente explotable del sistema.

CVE-2021-4140: Vulnerabilidad que posibilita construir un marcado XSLT específico que podría evadir una sandbox iframe.

Productos afectados
Firefox, versiones anteriores a Firefox 96.

Mitigación
Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces
https://www.mozilla.org/en-US/security/advisories/mfsa2022-01/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22746
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22743
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22744
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22741
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22740
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22738
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22737
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4140
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22745
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22744
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22747
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22736

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22739
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22752

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.01.13 12:09:29 -03'00'