Alerta de seguridad cibernética	9VSA21-00384-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero de 2021

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, CSIRT de Gobierno, comparte la información sobre vulnerabilidades entregada por Red Hat y que afectan a los paquetes Red Hat de Mozilla Thunderbird y a Red Hat Enterprise Linux.

Este informe incluye las medidas de mitigación, consistentes en instalar las actualizaciones de los productos afectados.

Vulnerabilidades

CVE-2020-15685

CVE-2020-26976

CVE-2021-23953

CVE-2021-23954

CVE-2021-23960

CVE-2021-23964

Impacto

Las vulnerabilidades consideradas de alto riesgo son las siguientes:

CVE-2021-23954: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. Se produce por un error de confusión de tipo de archivo al usar nuevos operadores lógicos en una instrucción switch de Java. Un atacante remoto puede crear una página web, engañar a la víctima para que la abra, detonar un error de confusión de tipo de archivo y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-23960: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. Se produce por haber validación insuficiente de las entradas hechas por los usuarios al realizar recolección de basura en variables JavaScript re-declaradas. Un atacante remoto puede crear una página web, engañar a la víctima para que la abra y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-23964: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. Se produce por un error de límites de la memoria al procesar contenido HTML. Un atacante remoto puede crear una página web, engañar a la víctima para que la abra y ejecutar código arbitrario en el sistema objetivo.

Productos afectados

Mozilla Thunderbird (Red Hat package): versiones 78.3.1-1.el8_1, a la 78.6.1-1.el8_1.
Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.1
Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.1
Red Hat Enterprise Linux Server - Update Services para SAP 8.1
Red Hat Enterprise Linux Server (para IBM Power LE) - Update Services para SAP 8.1.

Mitigación

Instalar las respectivas actualizaciones desde el sitio del proveedor.

Enlaces

https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/

https://www.mozilla.org/en-US/security/advisories/mfsa2021-04/

https://www.mozilla.org/en-US/security/advisories/mfsa2020-54/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15685

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26976

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23953

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23954

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23960

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23964

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.04 16:35:35 -03'00'