| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°022 | Fecha: 25-01-2024 |
|---|---|---|
| | | Página: 8 de 12 |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN NACIONAL DE INTELIGENCIA** | | |
| Nombre de la alerta | Actualización de SUSE para Mozilla Firefox | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Red, Internet | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |

Descripción

**1. ANTECEDENTES:**

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** y **MEDIA** de tipo escritura fuera de límites, desbordamiento de búfer, omisión de funciones de seguridad y advertencia de UI insuficiente sobre operaciones peligrosas de SUSE para Mozilla Firefox. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto comprometer el sistema afectado, realizar un ataque de clickjacking y ejecutar código arbitrario en el sistema de destino.

**2. DETALLES:**

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-0741 de tipo escritura fuera de límites, existe debido a un error de límite en ANGLE al procesar entradas que no son de confianza. Un atacante remoto puede engañar a la víctima para que abra un sitio web especialmente diseñado, provocar una escritura fuera de límites y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-0755 de tipo desbordamiento de búfer, existe debido a un error de límite al procesar contenido HTML. Un atacante remoto puede crear un sitio web especialmente diseñado, engañar a la víctima para que lo abra, provocar daños en la memoria y ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-0742 de tipo omisión de funciones de seguridad, existe debido a que no se actualiza la marca de tiempo ingresada por el usuario para ciertos mensajes y cuadros de diálogo del navegador. Un atacante remoto puede realizar un ataque de clickjacking y engañar a la víctima para que proporcione permisos no deseados a un sitio web malicioso.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-0750 de tipo advertencia de UI insuficiente sobre operaciones peligrosas, existe debido a un error en el cálculo del retraso de las notificaciones emergentes. Un atacante remoto puede realizar un ataque de clickjacking y engañar a un usuario para que otorgue permisos a una aplicación web maliciosa.

**A. Productos afectados:**

- SUSE Linux Enterprise Server para aplicaciones SAP 15: SP1.
- SUSE Linux Enterprise Server 15 SP1 LTSS: 15-SP1.
- SUSE Linux Enterprise Server 15: SP1.
- SUSE Linux Enterprise Computación de alto rendimiento 15 SP1 LTSS: 15-SP1.
- SUSE Linux Enterprise Computación de alto rendimiento 15: SP1.
- Plataforma SUSE CaaS: 4.0.
- Desarrollo de MozillaFirefox: anterior a 115.7.0-150000.150.122.1.
- MozillaFirefox-debuginfo: antes de 115.7.0-150000.150.122.1.
- MozillaFirefox: anterior a 115.7.0-150000.150.122.1.
- MozillaFirefox-traducciones-otras: anteriores a 115.7.0-150000.150.122.1.
- MozillaFirefox-traducciones-comunes: anteriores a 115.7.0-150000.150.122.1.
- MozillaFirefox-debugsource: anterior a 115.7.0-150000.150.122.1.

**3. RECOMENDACIÓN:**

- Actualizar los productos afectados de Mozilla Firefox a la última versión disponible que aborda estas vulnerabilidades.

| | |
|---|---|
| Fuente de Información: | • hxxp://www.suse.com/support/update/announcement/2024/suse-su-20240228-1/ |