USTIC-AV 05/22. Vulnerabilidades críticas en Mozilla Firefox y Thunderbird (24/05/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el CCN-CERT, avisa de la publicación de **dos vulnerabilidades**, catalogadas como **críticas, que afectan a**l navegador **Firefox y** al gestor de correo **Thunderbird, que permitirían la ejecución no autorizada de código JavaScript.**

Detalle

Mozilla ha publicado una aviso de seguridad (2022-19) que soluciona una serie de **vulnerabilidades** que **afectan al gestor de correo Thunderbird y** al **navegador Firefox, tanto en su versión de escritorio y soporte extendido (ESR)**, **como** en la versión para dispositivos **Android**. Estas aplicaciones se encuentran en uso en nuestra organización.

En la actualización se incluyen **2 vulnerabilidades** calificadas por el fabricante con una severidad **crítica que permitirían la ejecución remota de código JavaScript** en el sistema atacado. Se han asignado los identificadores **CVE-2022-1802 y CVE-2022-1529.** Estos errores fueron descubiertos por el investigador Manfred Paul a través de la Iniciativa Zero-Day de Trend Micro.

La base de datos del NIST, por el momento, no ha registrado estas vulnerabilidades, por lo tanto, no se les ha asignado puntuación de acuerdo con la escala CVSSv3. No obstante, Mozilla ha calificado estas vulnerabilidades como críticas**. Actualmente no se tiene conocimiento de reportes sobre actividad dañina en la red ni de la disponibilidad de *exploits* que aprovechen estas vulnerabilidades**, así como tampoco, se han publicado pruebas de concepto (PoC) sobre los detalles de los fallos publicados.

Debido a la criticidad, rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a la vulnerabilidad.

Recursos Afectados

- **Mozilla Firefox:** Versiones anterior a la 100.0.2
- **Mozilla for Android**: Versiones anteriores a la 100.3.0
- **Firefox ESR:** Versiones anteriores a la 91.9.1
- **Thunderbird**: Versiones anteriores a la 91.9.1

Recomendaciones Actualizadas (24/05/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos:

Mitigación

1º. Solución a las vulnerabilidades:

Se recomienda **actualizar** a la última versión disponible:

- Firefox 100.0.2
- Firefox ESR 91.9.1
- Firefox para Android 100.3
- Thunderbird 91.9.1.

2º. *Workaround* de la vulnerabilidad:

Por el momento, no se conocen medidas de mitigación alternativas para estas vulnerabilidades en caso de no ser posible aplicar las actualizaciones descritas.

Referencias

- Mozilla Foundation Security Advisory 2022-19
- Mozilla corrige dos problemas críticos de seguridad en Firefox y Thunderbird

En caso de haber detectado la explotación de esta vulnerabilidad :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indic ando en el *Asunto: [Compromiso Mozilla0522]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud