CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad en Productos Adobe Acrobat & Reader

Fecha: 03/08/2022

Problemática: Vulnerabilidad Use-After-Free (UAF) en productos Adobe Acrobat & Reader

Correlativo: AA-0007

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

La empresa Adobe Systems Incorporated alerta a todos sus usuarios sobre la vulnerabilidad Use-After-Free detectada en los productos Adobe Acrobat y Reader respectivamente, para que tomen las acciones necesarias para mitigar el problema detectado.

SITUACIÓN

El uso de memoria previamente liberada puede tener una serie de consecuencias adversas, que van desde la corrupción de datos válidos hasta la ejecución de código arbitrario por lo que:

- Si el área de memoria en cuestión se ha asignado y utilizado correctamente en otro lugar.
- Si la consolidación de fragmentos se produce después del uso de datos previamente liberados, el proceso puede bloquearse cuando se utilizan datos no válidos como información de fragmentos.
- Si se ingresan datos maliciosos antes de que pueda llevarse a cabo la consolidación de fragmentos, es posible aprovechar una primitiva de escribir qué y dónde para ejecutar código arbitrario.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

RECOMENDACIONES

Ante esta alerta, Adobe recomienda a sus usuarios que actualicen sus instalaciones de software a las últimas versiones siguiendo las recomendaciones para cada caso.

DICCIONARIO DE DATOS

1. Use-After-Free: Vulnerabilidad relacionada con el uso incorrecto de la memoria dinámica durante la operación del programa.
2. Aleatoriedad en la Disposición del Espacio de Direcciones (ASLR): Técnica de seguridad informática relacionada con la explotación de vulnerabilidades basadas en la corrupción de memoria.
3. Ejecución Arbitraria de Código: Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.

REFERENCIAS

1. https://helpx.adobe.com/security/products/acrobat/apsb22-32.html
2. https://nvd.nist.gov/vuln/detail/CVE-2022-34233#vulnCurrentDescriptionTitle
3. https://www.zscaler.es/blogs/security-research/analysis-adobe-acrobat-reader-javascript-docprint-use-after-free
4. https://cwe.mitre.org/data/definitions/416

ÁREA PARA DEFINICIONES

La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.

La presente herramienta tiene aplicación práctica derivado a un proceso previo de análisis con base al contexto y la situación del evento, sin embargo, se aclara que el presente sirve como guía y marco de referencia.