DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°217**	**Fecha: 14-09-2023**
		Página: 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Adobe lanzó actualización de seguridad que corrige una vulnerabilidad crítica en Adobe Acrobat y Reader para Windows y macOS		
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:

Adobe ha lanzado una actualización de seguridad que corrige una vulnerabilidad de severidad **CRÍTICA** de tipo escritura fuera de límites en Adobe Acrobat y Reader para Windows y macOS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-26369 en las versiones de Acrobat Reader 23.003.20284 (y anteriores), 20.005.30516 (y anteriores) y 20.005.30514 (y anteriores) se ven afectadas por una vulnerabilidad de escritura fuera de límites de la memoria que podría provocar la ejecución de código arbitrario en el contexto del usuario actual. La explotación de este problema requiere la interacción del usuario, ya que la víctima debe abrir un archivo malicioso.

Adobe indicó que esta vulnerabilidad está siendo explotada activamente en ataques que apuntan a Adoba Acrobat y Reader.

A. Productos afectados:

- Acrobat DC, versión 23.003.20284 y versiones anteriores (Windows y macOS);
- Acrobat Reader DC, 23.003.20284 y versiones anteriores (Windows y macOS);
- Acrobat 2020, versión 20.005.30516 (macOS) y 20.005.30514 (Windows) y versiones anteriores;
- Acrobat Reader 2020, 20.005.30516 (macOS) y 20.005.30514 (Windows) y versiones anteriores.

3. RECOMENDACIONES:

- Actualizar los productos afectados con las últimas versiones de software disponibles que abordan esta vulnerabilidad.
- Instalar las actualizaciones mediante su metodología preferida, como AIP-GPO, bootstrapper, SCUP/SCCM (Windows) o en macOS, Apple Remote Desktop y SSH.

Fuente de Información:	• hxxps://helpx.adobe.com/security/products/acrobat/apsb23-34.html • hxxps://helpx.adobe.com/security/products/connect/apsb23-33.html