DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°146**	**Fecha: 22-06-2023**
		Página: 17 de 23

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de ejecución remota de código en VMware vRealize Insight		
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

VMware Inc. ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección de comando en VMware Aria Operations for Networks (anteriormente VMware vRealize Network Insight) que viene siendo explotada en la naturaleza. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar un ataque de inyección de comandos que resulte en la ejecución remota de código.

2. DETALLES:

- **VMware Aria Operations for Networks**, es una herramienta de monitoreo de red que ayuda a las organizaciones a construir una infraestructura de red segura, optimizada y de alta disponibilidad.
- La vulnerabilidad de severidad **crítica** registrado como CVE-2023-20887 de tipo inyección de comando en Aria Operations for Networks podría permitir a un atacante remoto realizar un ataque de inyección de comandos que resulte en la ejecución remota de código.
- La vulnerabilidad de tipo inyección de comando se debe a que el producto construye la totalidad o una parte de un comando utilizando la entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente elementos especiales que podrían modificar el comando previsto cuando se envía a un componente descendente.
- Los investigadores indicaron que el código de explotación (PoC) para la vulnerabilidad CVE-2023-20887 está disponible en línea.

A. Productos afectados:

- VMware Aria Operations for Networks, versión 6.x.

3. RECOMENDACIONES:

- VMware recomienda actualizar el producto afectado con los últimos parches de firmware disponibles que abordan esta vulnerabilidad;
- Cabe indicar, que, a principios de junio, VMware lanzó parches de seguridad para abordar tres vulnerabilidades de severidad crítica y de alta gravedad, incluida la vulnerabilidad CVE-2023-20887;
- La empresa solucionó los problemas.
- as con el lanzamiento de VMware Aria Operations for Networks 6.x HF: KB92684.

Fuente de Información:	• hxxps://www.vmware.com/security/advisories/VMSA-2023-0012.html • hxxps://securityaffairs.com/147668/hacking/vmware-cve-2023-20887-flaw-attacks.html • hxxps://viz.greynoise.io/tag/vmware-aria-operations-for-networks-rce-attempt?days=30