Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°206**	**Fecha: 01-09-2023**
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Exploit lanzado para vulnerabilidad crítica de omisión de autenticación SSH de VMware		
Tipo de Ataque	Exploits	Abreviatura	Exploits
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Se ha publicado un código de explotación de prueba de concepto para una vulnerabilidad crítica de omisión de autenticación SSH en la herramienta de análisis Aria Operations for Networks de VMware (anteriormente conocida como vRealize Network Insight).

La falla (rastreada como CVE-2023-34039) fue encontrada por analistas de seguridad en ProjectDiscovery Research y parcheada por VMware el miércoles con el lanzamiento de la versión 6.11.

VMware Aria es una suite para administrar y monitorear entornos virtualizados y nubes híbridas, que permite la automatización de TI, la administración de registros, la generación de análisis, la visibilidad de la red, la planificación de seguridad y capacidad, y la administración de operaciones de alcance completo.

2. DETALLES:

La explotación exitosa permite a los atacantes remotos eludir la autenticación SSH en dispositivos sin parches y acceder a la interfaz de línea de comandos de la herramienta en ataques de baja complejidad que no requieren interacción del usuario debido a lo que la compañía describe como "una falta de generación de claves criptográficas únicas".

Para mitigar la falla, VMware "recomienda encarecidamente" aplicar parches de seguridad para las versiones 6.2 / 6.3 / 6.4 / 6.5.1 / 6.6 / 6.7 / 6.8 / 6.9 / 6.10 disponibles en el enlace hxxps://kb.vmware.com/s/article/94152

Hoy, VMware confirmó que el código de explotación CVE-2023-34039 se ha publicado en línea, dos días después de revelar el error de seguridad crítico.

El exploit de prueba de concepto (PoC) se dirige a todas las versiones de Aria Operations for Networks de 6.0 a 6.10, y fue desarrollado y lanzado por el investigador de vulnerabilidades de Summoning Team Sina Kheirkhah.

Kheirkhah dijo que la causa raíz del problema son las claves SSH codificadas que quedan después de que VMware olvidó regenerar las claves autorizadas SSH. "Cada versión de Aria Operations for Networks de VMware tiene una clave SSH única. Para crear un exploit completamente funcional, tuve que recopilar todas las claves de diferentes versiones de este producto", dijo Kheirkhah.

La vulnerabilidad de seguridad se corrigió en Aria Operations for Networks versión 6.11.0

VMware también parcheó una vulnerabilidad arbitraria de escritura de archivos esta semana (CVE-2023-20890), que permite a los atacantes obtener la ejecución remota de código después de obtener acceso de administrador al dispositivo objetivo (la PoC CVE-2023-34039 podría permitirles obtener permisos de root después de ataques exitosos).

En julio, VMware advirtió a los clientes que el código de explotación se lanzó en línea para una falla crítica de RCE (CVE-2023-20864) en la herramienta de análisis VMware Aria Operations for Logs, parcheada en abril.

Un mes antes, la compañía emitió otra alerta sobre la explotación activa de otro error crítico de Network Insight (CVE-2023-20887) que puede provocar ataques de ejecución de comandos remotos.

3. RECOMENDACIÓN:

- Actualizar sus dispositivos Aria Operations for Networks a la última versión lo antes posible: versión 6.11.0.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/exploit-released-for-critical-vmware-ssh-auth-bypass-vulnerability/ • hxxps://kb.vmware.com/s/article/94152