I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Omisión de autenticación SSH de VMware Aria y ejecución código remoto
Nivel de riesgo: Crítico

II. ALERTA

VMware lanzó actualizaciones de software para corregir dos vulnerabilidades de seguridad en Aria Operations for Networks que podrían explotarse para evitar la autenticación y obtener la ejecución remota de código.

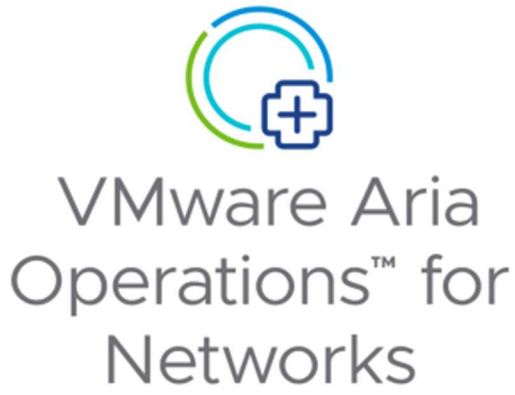

Figura No. 1.- Ilustración asociada a VMware Aria
Fuente: https://blogs.vmware.com/management/2023/02/announcing-vmware-aria-operations-for-networks-6-9.html

III. INTRODUCCIÓN

El 29 de agosto de 2023, fue publicado el CVE-2023-34039, relacionado con una vulnerabilidad de omisión de autenticación debido a la falta de generación de clave criptográfica única. Un atacante con acceso a la red de Aria Operations for Networks (anteriormente conocida como vRealize Network Insight) podría omitir la autenticación SSH para obtener acceso a la CLI de Aria Operations for Networks, se asignó una puntuación base de 9.8 crítica en el CVSS versión 3.1

La segunda vulnerabilidad, CVE-2023-20890 (puntuación CVSS: 7,2), es una vulnerabilidad de escritura de archivos arbitraria que afecta a Aria Operations for Networks y que podría ser utilizada por un atacante con acceso administrativo para escribir archivos en ubicaciones arbitrarias y lograr la ejecución remota de código.

IV. VECTOR DE ATAQUE:

Un atacante con acceso a la red de Aria Operations for Networks podría omitir la autenticación SSH para obtener acceso a la CLI de Aria Operations for Networks.

Versiones afectadas	Version Corregida	Documentación
VMware Aria Operations for Networks 6.X (6.2, 6.3, 6.4, 6.5.1, 6.6, 6.7, 6.8, 6.9 y 6.10)	6.11	Para versiones anteriores a la 6.11 se pueden utilizar los parches indicados en https://kb.vmware.com/s/article/94152

Tabla No. 1.- Versiones afectadas de VMware Aria Operations for Networks
Fuente: https://kb.vmware.com/s/article/94152

V. IMPACTO:

Exfiltración de información
Impacto Alto en la Confidencialidad, integridad y disponibilidad.

VI. INDICADORES DE COMPROMISO

No aplica

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Aplicar las actualizaciones provistas VMware.
- Eliminar archivos y cuentas de usuario no autorizados y restablecer las credenciales de la cuenta de servicio.
- Actualizar las reglas del firewall, para permitir únicamente conexiones a la infraestructura desde direcciones IP conocidas, configurar el firewall del sistema para bloquear el tráfico malicioso.
- Actualizar las políticas de acceso remoto para permitir solo conexiones entrantes desde direcciones IP conocidas y confiables.
- Consultar los avisos para CVE-2023-34039 y CVE-2023-20890 para aplicar los parches correspondientes.
- Mantener actualizado el software del sistema operativo y las aplicaciones, pero actuar con precaución al aplicar los parches de seguridad, y utilizar los más recientes siempre que sea posible.
- Monitorear de manera proactiva las relaciones de ejecución de procesos anormales y tomar medidas preventivas para evitar actividades como la exfiltración de información.

Con estas recomendaciones de seguridad, se puede minimizar las posibilidades de ser una víctima, las recomendaciones no garantizan la seguridad, pero ayudan a reducir el riesgo.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- *NVD - CVE-2023-34039*. (s. f.). https://nvd.nist.gov/vuln/detail/CVE-2023-34039
- *NVD - CVSS V3 Calculator*. (s. f.). https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2023-34039&vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H&version=3.1&source=VMware
- The Hacker News. (s. f.-a). *Critical vulnerability Alert: VMware Aria Operations networks at risk from remote attacks*. https://thehackernews.com/2023/08/critical-vulnerability-alert-vmware.html
- The Hacker News. (s. f.-b). *POC exploit released for critical VMware Aria's SSH Auth Bypass vulnerability*. https://thehackernews.com/2023/09/poc-exploit-released-for-critical.html
- *VMSA-2023-0018*. (2023, 30 agosto). VMware. https://www.vmware.com/security/advisories/VMSA-2023-0018.html
- *VMWare ArlA Operations for Networks Remote Code Execution ≈ Packet Storm*. (2023a, septiembre 2). https://packetstormsecurity.com/files/174452/VMWare-Aria-Operations-For-Networks-Remote-Code-Execution.html
- *VMWare ArlA Operations for Networks Remote Code Execution ≈ Packet Storm*. (2023b, septiembre 2). https://packetstormsecurity.com/files/174452/VMWare-Aria-Operations-For-Networks-Remote-Code-Execution.html
- *VMware Knowledge Base*. (s. f.). https://kb.vmware.com/s/article/94152