Se ha compartido código de explotación de prueba de concepto (PoC) para una reciente vulnerabilidad crítica, previamente divulgada y corregida, que afecta a VMware Aria Operations for Networks (anteriormente conocido como vRealize Network Insight).

Esta vulnerabilidad, identificada como CVE-2023-34039, tiene una calificación de severidad de 9.8 sobre un máximo de 10 y se ha descrito como un caso de omisión de autenticación debido a la ausencia de generación de claves criptográficas únicas.

> *«Un actor malicioso con acceso a la red de Aria Operations for Networks podría sortear la autenticación SSH para obtener acceso a la CLI de Aria Operations for Networks»,* anunció VMware a principios de esta semana.

Sina Kheirkhah del equipo Summoning, quien publicó la PoC después de analizar la corrección de VMware, explicó que la causa raíz puede rastrearse hasta un script bash que contiene un método llamado refresh_ssh_keys(), responsable de sobrescribir las claves SSH actuales para los usuarios de soporte y ubuntu en el archivo authorized_keys.

> *«Si bien existe una autenticación SSH, VMware olvidó regenerar las claves. VMware's Aria Operations for Networks había codificado sus claves desde la versión 6.0 hasta la 6.10»,* señaló Kheirkhah.

Las últimas correcciones de VMware también solucionan CVE-2023-20890, una vulnerabilidad de escritura arbitraria de archivos que afecta a Aria Operations for Networks y podría ser aprovechada por un atacante con acceso administrativo para escribir archivos en ubicaciones arbitrarias y lograr ejecución remota de código.

En otras palabras, un actor malicioso podría aprovechar la PoC para obtener acceso de administrador al dispositivo y explotar CVE-2023-20890 para ejecutar códigos arbitrarios, lo que resalta la importancia de que los usuarios apliquen las actualizaciones para protegerse

contra posibles amenazas.

La publicación de la PoC coincide con el gigante de la tecnología de virtualización emitiendo correcciones para una vulnerabilidad de alto riesgo de omisión de firma de token SAML (CVE-2023-20900, puntuación CVSS: 7.5) en varias versiones de VMware Tools para Windows y Linux.

> *«Un actor malicioso con posición de intermediario en la red (MITM) en la red de la máquina virtual podría eludir la verificación de firma de token SAML y llevar a cabo Operaciones de Invitado de VMware Tools»,* explicó la compañía en un comunicado emitido el jueves.

Peter Stöckli del Laboratorio de Seguridad de GitHub recibió el reconocimiento por informar sobre la vulnerabilidad, que afecta a las siguientes versiones:

- VMware Tools para Windows (12.x.x, 11.x.x, 10.3.x) – Corregido en 12.3.0
- VMware Tools para Linux (10.3.x) – Corregido en 10.3.26
- Implementación de código abierto de VMware Tools para Linux u open-vm-tools (12.x.x, 11.x.x, 10.3.x) – Corregido en 12.3.0 (será distribuido por proveedores de Linux)

Este desarrollo también se produce en un momento en que Fortinet FortiGuard Labs advierte sobre la continua explotación de vulnerabilidades de Adobe ColdFusion por parte de actores amenazantes para desplegar mineros de criptomonedas y bots híbridos como Satan DDoS (también conocido como Lucifer) y RudeMiner (también conocido como SpreadMiner), que son capaces de llevar a cabo ataques de criptojacking y ataques de denegación de servicio distribuido (DDoS).

Además, se ha implementado una puerta trasera llamada BillGates (también conocida como Setag), que es conocida por tomar el control de sistemas, robar información confidencial e iniciar ataques DDoS.