Várias vulnerabilidades nas operações do VMware Aria e nas ferramentas

Data: 2025-10-02 08:27:19

Autor: Inteligência Against Invaders

NÚMERO DO AVISO MS-ISAC:

2025-092

DATA(S) DE EMISSÃO:

09/30/2025

VISÃO GERAL:

Várias vulnerabilidades foram descobertas no VMware Aria Operations e no VMware Tools, a mais grave das quais pode permitir o escalonamento de privilégios para root. O VMware Aria é uma plataforma de gerenciamento multi-cloud que fornece automação, operações e gerenciamento de custos para aplicativos e infraestrutura em ambientes de nuvem privada, pública e híbrida. A exploração bem-sucedida da mais grave dessas vulnerabilidades pode permitir o escalonamento de privilégios para a raiz. Um invasor poderia então instalar programas; visualizar, alterar ou excluir dados; ou criar novas contas com direitos totais de usuário.

INTELIGÊNCIA DE AMEAÇAS:

NVISO indica que a vulnerabilidade CVE-2025-41244 foi explorada como um dia zero desde meados de outubro de 2024 pelo agente de ameaças vinculado à ChinaUNC5174.

SISTEMAS AFETADOS:

- Versões do VMware Cloud Foundation Operations anteriores à 9.0.1.0
- Versões do VMware Tools anteriores a 13.0.5.0, 13.0.5 e 12.5.4
- Versões do VMware Aria Operations anteriores à 8.18.5

RISCO:

Governo:

Grandes e médias entidades governamentaisALTO

Governo pequenoMÉDIA

Empresas:

Entidades de grandes e médias empresasALTO

Entidades de pequenas empresasMÉDIA

RESUMO TÉCNICO:

Várias vulnerabilidades foram descobertas no VMware Aria Operations e no VMware Tools, a mais grave das quais pode permitir o escalonamento de privilégios para root. Os detalhes da vulnerabilidade são os seguintes:

Tática: *Escalonamento de privilégios* (TA0004):

Técnica: *Exploração para escalonamento de privilégios* (T1068):

- Um ator local mal-intencionado com privilégios não administrativos que tenha acesso a uma VM com o VMware Tools instalado e gerenciado pelo Aria Operations com o SDMP ativado pode explorar essa vulnerabilidade para escalar privilégios para root na mesma VM. (CVE-2025-41244)

- Um agente mal-intencionado com privilégios não administrativos no Aria Operations pode explorar essa vulnerabilidade para divulgar credenciais de outros usuários do Aria Operations. (CVE-2025-41245)
- Um ator mal-intencionado com privilégios não administrativos em uma VM convidada, que já está autenticada por meio do vCenter ou do ESX, pode explorar esse problema para acessar outras VMs convidadas. A exploração bem-sucedida requer conhecimento das credenciais das VMs de destino e do vCenter ou ESX. (CVE-2025-41246)

A exploração bem-sucedida da mais grave dessas vulnerabilidades pode permitir o escalonamento de privilégios para a raiz. Um invasor poderia então instalar programas; visualizar, alterar ou excluir dados; ou criar novas contas com direitos totais de usuário.

RECOMENDAÇÕES:

Recomendamos que as seguintes ações sejam tomadas:

- Aplique as atualizações apropriadas fornecidas pela Broadcom ou por outros fornecedores que usam este software a sistemas vulneráveis imediatamente após o teste apropriado. (**M1051: Atualizar software**)
- **Salvaguarda 7.1 : Estabelecer e manter um processo de gerenciamento de vulnerabilidades:** Estabeleça e mantenha um processo documentado de gerenciamento de vulnerabilidades para ativos corporativos. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar esta Salvaguarda.
- **Salvaguarda 7.2: Estabelecer e manter um processo de correção:**Estabeleça e mantenha uma estratégia de correção baseada em risco documentada em um processo de correção, com revisões mensais ou mais frequentes.
- **Safeguard 7.4: Execute o gerenciamento automatizado de patches de aplicativos:**Execute atualizações de aplicativos em ativos corporativos por meio do gerenciamento automatizado de patches mensalmente ou com mais frequência.
- **Salvaguarda 7.5: Executar verificações automatizadas de vulnerabilidade de ativos corporativos internos:** Execute verificações automatizadas de vulnerabilidades de ativos corporativos internos trimestralmente ou com mais frequência. Realize verificações autenticadas e não autenticadas, usando uma ferramenta de verificação de vulnerabilidades compatível com SCAP.
- **Salvaguarda 7.7: Corrigir vulnerabilidades detectadas:**Corrija vulnerabilidades detectadas no software por meio de processos e ferramentas mensalmente ou com mais frequência, com base no processo de correção.
- **Salvaguarda 12.1: Garantir que a infraestrutura de rede esteja atualizada:**Certifique-se de que a infraestrutura de rede seja mantida atualizada. Exemplo de implementaçãoOs programas incluem a execução da versão estável mais recente do software e/ou o uso de ofertas de rede como serviço (NaaS) atualmente suportadas. Revise as versões do software mensalmente, ou com mais frequência, para verificar o suporte ao software.
- **Salvaguarda 18.1: Estabelecer e manter um programa de teste de penetração:**Estabelecer e manter um programa de teste de penetração apropriado ao

tamanho, complexidade e maturidade da empresa. As características do programa de teste de penetração incluem escopo, como rede, aplicativo Web, Interface de Programação de Aplicativos (API), serviços hospedados e controles de instalações físicas; frequência; limitações, como horas aceitáveis e tipos de ataque excluídos; informações de ponto de contato; correção, como a forma como as descobertas serão roteadas internamente; e requisitos retrospectivos.

- **Salvaguarda 18.2: Executar testes periódicos de penetração externa:**Realize testes periódicos de penetração externa com base nos requisitos do programa, pelo menos anualmente. O teste de penetração externa deve incluir reconhecimento corporativo e ambiental para detectar informações exploráveis. O teste de penetração requer habilidades e experiência especializadas e deve ser conduzido por uma parte qualificada. O teste pode ser uma caixa transparente ou uma caixa opaca.
- **Salvaguarda 18.3: Corrigir resultados do teste de penetração:**Corrija as descobertas do teste de penetração com base na política da empresa para escopo e priorização de correção.

- Aplique o Princípio do Menor Privilégio a todos os sistemas e serviços. Execute todos os softwares como um usuário sem privilégios (sem privilégios administrativos) para diminuir os efeitos de um ataque bem-sucedido. (**M1026: Gerenciamento de contas privilegiadas**)
- **Salvaguarda 4.7: Gerenciar contas padrão em ativos e software corporativos:**Gerencie contas padrão em ativos e software corporativos, como raiz, administrador e outras contas de fornecedores pré-configuradas. Exemplos de implementações podem incluir: desabilitar contas padrão ou torná-las inutilizáveis.
- **Salvaguarda 5.5: Estabelecer e manter um inventário de contas de serviço:**Estabeleça e mantenha um inventário de contas de serviço. O inventário, no mínimo, deve conter o proprietário do departamento, a data de revisão e a finalidade. Execute revisões de conta de serviço para validar se todas as contas ativas estão autorizadas, em uma agenda recorrente no mínimo trimestralmente ou com mais frequência.

- A verificação de vulnerabilidades é usada para encontrar vulnerabilidades de software potencialmente exploráveis para corrigi-las. (**M1016**:**Verificação de vulnerabilidades**)
- **Salvaguarda 16.13: Realizar Teste de Penetração de Aplicativos:**Realize testes de penetração de aplicativos. Para aplicativos críticos, o teste de penetração autenticado é mais adequado para encontrar vulnerabilidades de lógica de negócios do que a verificação de código e o teste de segurança automatizado. O teste de penetração depende da habilidade do testador de manipular manualmente um aplicativo como um usuário autenticado e não autenticado.

- Arquitetar seções da rede para isolar sistemas, funções ou recursos críticos. Use segmentação física e lógica para impedir o acesso a sistemas e informações potencialmente confidenciais. Use uma DMZ para conter todos os serviços voltados para a Internet que não devem ser expostos da rede interna. Configure instâncias separadas de nuvem privada virtual (VPC) para isolar sistemas de nuvem críticos. (**M1030**:**Segmentação de rede**)
- **Salvaguarda 12.2: Estabelecer e manter uma arquitetura de rede segura:** Estabeleça e mantenha uma arquitetura de rede segura. Uma arquitetura de rede segura deve abordar a segmentação, o menor privilégio e a disponibilidade, no mínimo.

- Use recursos para detectar e bloquear condições que possam levar ou ser indicativas da ocorrência de uma exploração de software. (**M1050**:**Proteção contra exploits**)
- **Salvaguarda 10.5:Ative os recursos anti-exploração:**Habilite recursos antiexploração em ativos e software corporativos, sempre que possível, como® Microsoft Data Execution

Prevention (DEP), Windows® Defender Exploit Guard (WDEG) ou Apple® System Integrity Protection (SIP) e Gatekeeper™.