TLP: CLEAR

BOLETIM DE SEGURANÇA

Broadcom corrige falhas no VMware Aria que resultavam em roubo de credenciais

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

SUMÁRIO

1 INTRODUÇÃO EXECUTIVA

Recentemente, foram identificadas e corrigidas cinco vulnerabilidades significativas nos produtos **VMware Aria Operations** e **VMware Aria Operations for Logs**. Essas falhas poderiam permitir que agentes mal-intencionados obtenham acesso elevado ou informações sensíveis, comprometendo a segurança dos sistemas afetados.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

Segue abaixo a lista de vulnerabilidades identificadas e informadas pela VMware, acompanhadas de uma breve descrição de cada uma. Essas informações são essenciais para compreender os riscos associados e tomar as medidas necessárias para mitigar possíveis impactos.

CVE-2025-22218

- Uma vulnerabilidade de divulgação de informações no VMware Aria Operations for Logs. Atores de ameaças com permissões de "View Only Admin" pode ler as credenciais de um produto VMware integrado ao Aria Operations for Logs.

CVE-2025-22219

- Falha de cross-site scripting (XSS) armazenado no VMware Aria Operations for Logs. Um ator com privilégios não administrativos pode injetar um script malicioso que pode levar a operações arbitrárias como usuário administrador.

CVE-2025-22220

- Vulnerabilidade de escalonamento de privilégios no VMware Aria Operations for Logs. Um ator com privilégios não administrativos e acesso à API do Aria Operations for Logs pode realizar certas operações no contexto de um usuário administrador.

CVE-2025-22221

- Vulnerabilidade de cross-site scripting (XSS) armazenado no VMware Aria Operations for Logs. Um ator com privilégios administrativos pode injetar um script malicioso que pode ser executado no navegador da vítima ao realizar uma ação de exclusão na Configuração do Agente.

CVE-2025-22222

- Uma falha de divulgação de informações no VMware Aria Operations. Um usuário com privilégios não administrativos pode explorar essa vulnerabilidade para recuperar credenciais de um plugin de saída se um ID de credencial de serviço válido for conhecido.

2.1 SISTEMAS E PRODUTOS AFETADOS

A vulnerabilidade afeta as seguintes ferramentas e versões:

- *VMware Aria Operations for Logs, versões anteriores à 8.18.3*
- *VMware Aria Operations, versões anteriores à 8.18.3*
- *VMware Cloud Foundation, versões 5.x, 4.x*

2.2 IMPACTO DA VULNERABILIDADE

Os impactos das vulnerabilidades identificadas nos produtos VMware Aria Operations e VMware Aria Operations for Logs incluem:

- *Divulgação de informações sensíveis*
- *Execução remota de código via Cross-Site Scripting*
- *Escalonamento de privilégios*

3 RECOMENDAÇÕES

Para mitigar os riscos associados às vulnerabilidades identificadas nos produtos VMware Aria Operations e Aria Operations for Logs, é fundamental adotar medidas preventivas. Recomenda-se, como ação prioritária:

Aplicação imediata dos patches de segurança

- VMware Aria Operations for Logs, versões 8.18.3 ou superior
- VMware Aria Operations versões, 8.18.3 ou superior
- VMware Cloud Foundation, KB92148

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Broadcom**
- **NVD**
- **The Hacker News**

5 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH