Um bug crítico no VMware Aria Operations e no VMware Tools foi explorad

Data: 2025-10-01 14:22:23

Autor: Inteligência Against Invaders

Redazione RHC**:1 Outubro 2025 15:56**

A Broadcom corrigiu uma vulnerabilidade grave de escalonamento de privilégios em **Operações do VMware Aria e ferramentas VMware** que foi explorado em ataques a partir de outubro de 2024. O problema recebeu o identificador CVE-2025-41244. Embora a empresa não tenha relatado uma exploração no oficial boletim , o pesquisador da NVISO Maxime Thibault reportado em maio, que os ataques começaram em meados de outubro de 2024. A análise ligou os ataques ao grupo chinês **UNC5174** .

A vulnerabilidade permite que um usuário local sem privilégios *injetar um binário malicioso em diretórios que correspondem a expressões regulares genéricas* . Uma variante observada em ataques do mundo real usa o diretório /tmp/httpd. Para que o malware seja detectado pelo serviço VMware, **Ele deve ser executado como um usuário normal e abrir um soquete de rede aleatório.**

Como resultado, os invasores ganham a capacidade de *escalar privilégios de root e executar código arbitrário dentro da máquina virtual.* A NVISO também publicou uma exploração de demonstração mostrando como essa falha pode ser usada para comprometer o VMware Aria Operations no modo credenciado e o VMware Tools no modo não credenciado.

De acordo com o Google Mandiant, a UNC5174 opera em nome do Ministério da Segurança do Estado da China. Em 2023, o grupo vendeu acesso às redes de empreiteiros de defesa dos EUA, agências governamentais britânicas e organizações asiáticas, explorando o CVE-2023-46747 vulnerabilidade no F5 BIG-IP.

Em fevereiro de 2024, eles exploraram o CVE-2024-1709 vulnerabilidade em **ConnectWise ScreenConnect,** atacando centenas de instituições nos Estados Unidos e Canadá.

Na primavera de 2025, o grupo também foi observado explorando o CVE-2025-31324 vulnerabilidade, um erro de upload de arquivo em **NetWeaver Visual Composer** que permitia a execução de código arbitrário. Outros grupos chineses também participaram de ataques a sistemas SAP, incluindo Chaya_004, UNC5221 e CL-STA-0048, que instalaram backdoors em mais de 580 instâncias do NetWeaver, incluindo aquelas em infraestrutura crítica nos Estados Unidos e no Reino Unido.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli