Broadcom emite patches para falhas de segurança do VMware NSX e vCen

Data: 2025-10-02 10:16:54

Autor: Inteligência Against Invaders

Um conjunto de atualizações de segurança substanciais para VMware NSX e vCenter foi lançado pela Broadcom, abordando várias vulnerabilidades de alta gravidade que podem expor os sistemas corporativos a ataques cibernéticos.

As falhas, divulgadas nas últimas atualizações do VMware vCenter e NSX, abordam várias vulnerabilidades (CVE-2025-41250, CVE-2025-41251, CVE-2025-41252), que foram relatadas pela Agência de Segurança Nacional dos EUA e pesquisadores de segurança independentes.

Eles afetam vários produtos da Broadcom, incluindo VMware Cloud Foundation, NSX-T e VMware Telco Cloud Platform.

Um dos problemas mais graves, rastreado como CVE-2025-41250, é um bug de injeção de cabeçalho SMTP no vCenter. Com uma pontuação básica CVSSv3 de 8,5, ele permite que invasores com privilégios não administrativos modifiquem as notificações por e-mail associadas a tarefas agendadas. A Broadcom disse que não há soluções alternativas disponíveis e os usuários devem aplicar as versões corrigidas imediatamente.

Duas outras falhas no VMware NSX, CVE-2025-41251 e CVE-2025-41252, decorrem de pontos fracos no processo de autenticação. Ambos permitem que invasores não autenticados enumerem nomes de usuário válidos, uma etapa que pode suportar tentativas de login não autorizadas ou de força bruta.

“Com base nas informações disponíveis, essas vulnerabilidades podem ser combinadas para criar um caminho de ataque viável do reconhecimento não autenticado para o comprometimento autenticado”, disse Mayuresh Dani, gerente de pesquisa de segurança da Qualys Threat Research Unit.

“Uma vez autenticados (considerando privilégios limitados), os agentes de ameaças explorarão a injeção de cabeçalho SMTP do vCenter para redirecionar potencialmente a comunicação confidencial e aumentar seus privilégios.”

Leia mais sobre gerenciamento de patches de segurança cibernética: Sete etapas para criar um programa maduro de gerenciamento de vulnerabilidades

As vulnerabilidades são classificadas como “Altas” com pontuações CVSS variando de 7,5 a 8,5. Os pontos fracos afetam uma ampla gama de soluções de infraestrutura VMware usadas em ambientes corporativos e de telecomunicações.

De acordo com a Broadcomadvisory, os seguintes produtos são afetados:

- VMware NSX
- NSX-T
- Fundação VMware Cloud
- VMware vCenter Server
- Plataforma de nuvem VMware Telco
- Infraestrutura de nuvem de telecomunicações da VMware

“Os dois bugs do NSX permitem que usuários não autenticados confirmem quais nomes de usuário existem em um sistema”, explicou Jason Soroko, membro sênior da Sectigo.

“Mesmo sem a execução direta do código, esses tipos de falhas são blocos de construção atraentes que os adversários combinam com credenciais fracas ou reutilizadas para se aprofundar, o que ajuda a explicar por que uma agência de inteligência os sinalizaria apesar das classificações altas, em vez de críticas.”

Divulgação mais ampla

Juntamente com esses patches, a Broadcom também revelou três outras vulnerabilidades no VMware Aria Operations e no VMware Tools.

Essas falhas (CVE-2025-41244, CVE-2025-41245, CVE-2025-41246) podem permitir que os invasores escalem privilégios para root, roubem credenciais ou acessem VMs convidadas.

“A última vez que a NSA relatou vulnerabilidades do VMware foi quando atores patrocinados pelo Estado russo as exploraram ativamente”, observou Dani, referindo-se a CVE-2020-4006.

“Isso sugere que a agência pode ter inteligência indicando potencial interesse de exploração de atores do estado-nação.”

No momento da publicação, Soroko esclareceu: “Não há confirmação pública de que os bugs de enumeração de nome de usuário do NSX ou a injeção de cabeçalho SMTP do vCenter foram explorados na natureza”.

Ainda assim, os administradores são instados a atualizar os sistemas afetados o mais rápido possível para mitigar os riscos. Versões fixas e documentação estão disponíveis no site de suporte da Broadcom.