Falha crítica do SAP S/4HANA CVE-2025-42957 sob exploração ativa

Data: 2025-09-05 20:47:56

Autor: Inteligência Against Invaders

Falha crítica do SAP S/4HANA CVE-2025-42957 sob exploração ativa

Especialistas alertam para uma vulnerabilidade explorada ativamente, rastreada comoCVE-2025-42957(pontuação CVSS: 9,9), no software SAP S/4HANA.

Uma vulnerabilidade crítica de injeção de comando, rastreada como **CVE-2025-42957** (pontuação CVSS de 9,9), no SAP S/4HANA está sob exploração ativa.

Um invasor pode explorar essa falha para comprometer totalmente os sistemas SAP, alterando bancos de dados, criando contas de superusuário e roubando hashes de senha.

“O SAP S/4HANA permite que um invasor com privilégios de usuário explore uma vulnerabilidade no módulo de função exposto via RFC. Essa falha permite a injeção de código ABAP arbitrário no sistema, ignorando verificações de autorização essenciais.” lê o comunicado*. “Essa vulnerabilidade funciona efetivamente como um backdoor, criando o risco de comprometimento total do sistema, minando a confidencialidade, integridade e disponibilidade do sistema.”*

O SAP S/4HANA ERP é o pacote de planejamento de recursos empresariais (ERP) da SAP, projetado para ajudar organizações de grande e médio porte a gerenciar os principais processos de negócios, como finanças, cadeia de suprimentos, manufatura, vendas, compras e recursos humanos.

A falha afeta todas as versões do SAP S/4HANA (nuvem privada e local) e pode ser explorada a partir de uma conta de baixo privilégio para comprometer totalmente o sistema.

O fornecedor abordou a vulnerabilidade em 11 de agosto de 2025.

O SecurityBridge Threat Research Labs encontrou e confirmou uma exploração para esse problema que está ativa na natureza, recomendando que os administradores resolvam imediatamente a falha.

“Um comprometimento completo do sistema com o mínimo de esforço necessário, onde a exploração bem-sucedida pode facilmente levar a fraudes, roubo de dados, espionagem ou instalação de ransomware.” relatou SecurityBridge*. “Para demonstrar o impacto potencial dessa vulnerabilidade, criamos a demonstração anexa com base em nossa própria pesquisa e ferramentas:”*

[VÍDEO/IFRAME REMOVIDO]

Os especialistas da SecurityBridge alertam que, embora ainda não seja generalizada, a falha já está sendo abusada. Os sistemas SAP sem patch são expostos e os exploits são fáceis de criar por meio da engenharia reversa do patch ABAP.

“O invasor precisa apenas de credenciais de baixo nível no sistema SAP (qualquer conta de usuário válida com permissões para chamar o módulo RFC vulnerável e a autorização de S_DMIS específica com a atividade 02), e nenhuma interação do usuário é necessária”, conclui a SecurityBridge.

*“A complexidade do ataque é baixa e pode ser realizada pela rede, e é por isso que a pontuação CVSS é tão alta (9,9). Em resumo, um insider mal-intencionado ou um agente de ameaça que obteve acesso básico de usuário (por meio de phishing, por exemplo) poderiaaproveitar essa falha para**escalar para o controle total do ambiente SAP**.“*

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,SAP S/4HANA)