As falhas do Suse Rancher permitem que os atacantes bloqueem contas d

Data: 2025-09-29 08:05:22

Autor: Inteligência Against Invaders

Foi descoberto um gerente crítico de insutação de insucedores de vulnerabilidades de segurança

que permite que os invasores com privilégios elevados bloqueem contas administrativas,

potencialmente interrompendo Cluster de Kubernetes operações de gerenciamento.

A falha, rastreada ASCVE-2024-58260, possui uma classificação de alta gravidade com uma pontuação CVSS de 7,1.

Visão geral da vulnerabilidade

O problema de segurança decorre da validação do lado do servidor ausente no campo de nome de usuário do Rancher Manager.

Essa supervisão permite que os usuários com permissões de atualização sobre os recursos do usuário manipulem nomes de usuário de maneiras que podem negar o acesso ao serviço a contas direcionadas, incluindo a conta de administrador crítica.

Atributo	Detalhes
Cve id	CVE-2024-58260
Gravidade	High (CVSS 7.1)
Vetor CVSS	CVSS: 3.1/av: n/ac: l/pr: h/ui: n/s: c/c: n/i: l/a: h
Versões remendadas	2.12.2, 2.11.6, 2.10.10, 2.9.12

A vulnerabilidade permite dois vetores de ataque primário. Ataques de aquisição do nome InUserning, usuários maliciosos podem definir o nome de usuário de outro usuário como “Admin”, impedindo que o administrador legítimo e o usuário afetado efetuem login devido à aplicação da singularidade do fazendeiro no tempo de login.

Além disso, o bloqueio de contas ataca usuários com permissões de atualização em contas de administrador para alterar o nome de usuário do administrador, bloqueando efetivamente a todos Acesso administrativo para a interface do usuário do fazendeiro.

Esses cenários de ataque estão alinhados com o Mitre ATT & CK Framework’s Access Access RemovalTechnique (T1531), onde os adversários interrompem a disponibilidade de recursos do sistema e da rede, inibindo o acesso às contas utilizadas por usuários legítimos.

A falha afeta especificamente as organizações que executam versões de gerente de fazendas afetadas em várias filiais de liberação.

A vulnerabilidade requer altos privilégios para explorar, pois os invasores já devem possuir permissões de atualização sobre os recursos do usuário.

No entanto, uma vez explorado, o impacto pode ser grave, interrompendo completamente os recursos de administração da plataforma e autenticação do usuário.

As organizações devem atualizar imediatamente para versões corrigidas: 2.12.2,2.11.6.2.10.10, OR2.9.12.

Para ambientes em que o patch imediato não é viável, os administradores devem limitar estritamente as permissões de atualização sobre recursos relacionados ao usuário a apenas usuários confiáveis.

A divulgação de vulnerabilidade foi Published Pelo pesquisador de segurança Samjustus através do Github Security Advisory GHSA-Q82V-H4RQ-5C86, enfatizando a importância da validação de entrada adequada nas plataformas de gerenciamento de contêineres corporativos.