

Erro ao acessar serviço SSH

01/07/2025 18:10:45

[Imprimir artigo da FAQ](#)

Categoria:	Redes::Serviços de Rede	Votos:	0
Estado:	público (todos)	Resultado:	0.00 %
Idioma:	pt_BR	Última atualização:	Qui 12 Mai 18:40:51 2022

Palavras-chave

negotiate key exchange sha1 diffie-hellman

Sintoma (público)

Ao tentar acessar um dispositivo via SSH é exibida as possíveis mensagens:

Unable to negotiate with x.x.x.x port xx: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,diffie-hellman-group-exchange-sha1

Unable to negotiate with x.x.x.x port xx: no matching cipher found. Their offer: aes128-cbc,3des-cbc,des-cbc

Problema (público)

Versão incompatível entre o cliente e o servidor SSH.

Nesse caso, o cliente e o servidor não conseguiram concordar com o algoritmo de troca de chaves. O servidor oferecia apenas um único método diffie-hellman-group1-sha1. O OpenSSH suporta esse método, mas não o habilita por padrão porque é fraco e está dentro do alcance teórico do chamado ataque Logjam.

Solução (público)