某局点 S6520X-EI设备扫描出漏洞CVE-2002-20001

SSH　刘倩　2022-08-24 发表

问题描述

如题目

解决方法

规避方法：Key exchange algorithms不使用dh相关算法

[2015]ssh2 algorithm key-exchange ?

dh-group-exchange-sha1	Diffie-Hellman-group-exchange-SHA1
dh-group1-sha1	Diffie-Hellman-group1-SHA1
dh-group14-sha1	Diffie-Hellman-group14-SHA1
ecdh-sha2-nistp256	Elliptic Curve Diffie-Hellman-SHA2-256
ecdh-sha2-nistp384	Elliptic Curve Diffie-Hellman-SHA2-384

比如

[2.14]ssh2 algorithm key-exchange ecdh-sha2-nistp256