

CiscoPIX欺骗TCPSYN报文拒绝服务漏洞 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/181/2021_2022_CiscoPIX_E6_AC_c101_181613.htm 受影响系统：Cisco PIX Firewall 7.0

Cisco PIX Firewall 6.3 详细描述：Cisco PIX是一款硬件防火墙解决方案。Cisco PIX在处理畸形的TCP报文时存在漏洞，远程攻击者可能利用此漏洞对合法源访问进行拒绝服务攻击。如果通过PIX防火墙发送了有错误校验和的TCP SYN报文的话，PIX就会阻断使用相同源和目标TCP端口及IP地址的新TCP连接，直到30秒后才会允许新的连接。因此攻击者可以发送有错误校验和的特制TCP报文，将源/目标IP和端口设置为合法的主机。一旦PIX防火墙接收了这样的报文，就无法同恶意报文中所指定的凭据建立新的TCP会话，默认时间为7.0版为30秒，6.3版为2分2秒，之后会恢复正常运行。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com