

知

OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)

漏洞相关

王奎银

2022-01-07 发表

漏洞相关信息

漏洞编号： CVE-2008-5161

漏洞名称： OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)

产品型号及版本： 防火墙、负载均衡、入侵防御

漏洞描述

OpenSSH是一种开放源码的SSH协议的实现，初始版本用于OpenBSD平台，现在已经被移植到多种Unix/Linux类操作系统下。如果配置为CBC模式的话，OpenSSH没有正确地处理分组密码算法加密的SSH会话中所出现的错误，导致可能泄露密文中任意块最多32位纯文本。在以标准配置使用OpenSSH时，攻击者恢复32位纯文本的成功概率为 2^{-18} ，此外另一种攻击变种恢复14位纯文本的成功概率为 2^{-14} 。

漏洞解决方案

Comware平台及iware平台都不涉及该漏洞。

