

# 知 Workspace是否涉及OpenSSH相关漏洞CVE-2019-16905&CVE-2020-15778 &CVE-2021-28041&CVE-2018-15473&CVE-2018-15919&CVE-2018-20685

戴丽丽 2021-08-23 发表

## 漏洞相关信息

漏洞编号: CVE-2019-16905/CVE-2020-15778/CVE-2021-28041/CVE-2018-15473/CVE-2018-15919/CVE-2018-20685

漏洞名称: OpenSSH相关漏洞

产品型号及版本: E1009

## 漏洞描述

### 1、OpenSSH 输入验证错误漏洞(CVE-2019-16905)

OpenSSH 7.7版本至7.9版本和8.1之前的8.x版本中存在输入验证错误漏洞。

### 2、OpenSSH 操作系统命令注入漏洞(CVE-2020-15778)

OpenSSH 8.3p1及之前版本中的scp的scp.c文件存在操作系统命令注入漏洞。

### 3、OpenSSH 资源管理错误漏洞(CVE-2021-28041)

OpenSSH before 8.5 存在安全漏洞，攻击者可利用该漏洞在遗留操作系统上不受约束的代理套接字访问。

### 4、OpenSSH 竞争条件问题漏洞(CVE-2018-15473)

OpenSSH 7.7及之前版本中存在竞争条件问题漏洞。

### 5、OpenSSH 信息泄露漏洞(CVE-2018-15919)

OpenSSH 7.8及之前版本中的auth-gss2.c文件存在信息泄露漏洞。

### 6、OpenSSH 访问控制错误漏洞(CVE-2018-20685)

OpenSSH 7.9版本中的scp客户端的scp.c文件存在安全漏洞。

#### 漏洞解决方案

在E1009环境中使用ssh -V查询openssh版本为7.4p1，存在上述漏洞，E1010版本openssh版本已经更新至8.5p1，不存在上述漏洞。

