[通用漏洞编号：CVE-2016-10009]

知道创宇漏洞速递

KNOWNSEC VULNERABILITIES EXPRESS DELIVERY

OpenSSH远程代码执行漏洞

知道创宇

北京知道创宇信息技术有限公司

漏洞名称：OpenSSH 远程代码执行漏洞

1.漏洞情况分析

通用漏洞编号：CVE-2016-10009

OpenSSH 近日紧急发布了 7.4 版本，该版本中修复了一个远程代码执行漏洞，该漏洞发生在 ssh-agent 中，加载模块的请求可通过代理进行转发，攻击者可能会尝试在转发时加载一个不兼容的 PKCS#11 模块，该模块是共享库，如果攻击者控制了转发的 agent-socket（即运行 sshd 服务的主机），会导致在运行 ssh-agent（通常是运行 ssh 的客户端）的系统上执行代码并向系统写文件的能力。

除该漏洞外，该版本还修复了：

CVE-2016-10010

当关闭 UsePrivilegeSeparation 权限隔离功能时，ssh 转发的 socket 文件将以 root 权限创建；

CVE-2016-10011

sshd 创建的子进程被攻击者提权后，主机的私钥会通过 realloc()泄露；

CVE-2016-10012

sshd 服务器启用认证前压缩（Compression yes）可能导致攻击者从经过权限隔离的子进程中攻击高权限的父进程。

2.漏洞影响范围

影响版本：

OpenSSH OpenSSH 7.3

OpenSSH OpenSSH 7.2p2

OpenSSH OpenSSH 7.2

OpenSSH OpenSSH 7.1p2

OpenSSH OpenSSH 7.1p1

OpenSSH OpenSSH 7.1

OpenSSH OpenSSH 7.0

OpenSSH OpenSSH 6.9p1

OpenSSH OpenSSH 6.9

OpenSSH OpenSSH 6.6

OpenSSH OpenSSH 6.5

OpenSSH OpenSSH 6.4

OpenSSH OpenSSH 6.3

OpenSSH OpenSSH 6.2

OpenSSH OpenSSH 6.1

OpenSSH OpenSSH 6.0

OpenSSH OpenSSH 5.8

OpenSSH OpenSSH 5.7

OpenSSH OpenSSH 5.6

OpenSSH OpenSSH 5.5

OpenSSH OpenSSH 5.4

OpenSSH OpenSSH 5.3

OpenSSH OpenSSH 5.2

OpenSSH OpenSSH 5.1

OpenSSH OpenSSH 5.0

不受影响版本：

OpenSSH OpenSSH 7.4

3.漏洞修复建议

升级至 OpenSSH OpenSSH 7.4

4.相关链接

http://www.securityfocus.com/bid/94968/info

http://www.openssh.com/txt/release-7.4