CSAP-SA openssh漏洞问题

漏洞相关 孔德飞 2022-07-14 发表

漏洞相关信息

漏洞编号： openssh相关漏洞

漏洞名称： openssh相关漏洞

产品型号及版本： CSAP-SA

漏洞描述

openssh相关漏洞

OpenSSH挑战响应(Challenge-Response)机制交互键盘PAM验证远程缓冲区错误漏洞(CVE-2002-0639)
OpenSSH挑战响应(Challenge-Response)机制交互键盘PAM验证远程缓冲区错误漏洞(CVE-2002-0640)
OpenSSH缓冲区管理操作远程溢出漏洞(CVE-2003-0693)
OpenSSH 任意命令执行漏洞(CVE-2006-5051)
Diffie-Hellman Key Agreement Protocol 资源管理错误漏洞(CVE-2002-20001)
OpenSSH Kerberos 4 TGT/AFS令牌缓冲区错误漏洞(CVE-2002-0575)
OpenBSD sshd BSD验证实现错误漏洞(CVE-2002-0765)
SSH Communications SSH AllowedAuthentications配置存在漏洞(CVE-2002-1646)
OpenSSH远程客户端地址限制可绕过漏洞(CVE-2003-0386)
OpenSSH漏洞(CVE-2003-0682)
OpenSSH 缓冲区管理错误漏洞(CVE-2003-0695)
OpenSSH sshd Privilege Separation Monitor 未明漏洞(CVE-2006-5794)
OpenSSH J-PAKE授权问题漏洞(CVE-2010-4478)
OpenSSH'hash_buffer'函数缓冲区错误漏洞(CVE-2014-1692)
OpenSSH sshd 权限许可和访问控制问题漏洞(CVE-2015-5600)
OpenSSH sshd 安全漏洞(CVE-2015-8325)
OpenSSH 代码问题漏洞(CVE-2016-10009)
OpenSSH sshd 安全漏洞(CVE-2016-10010)
OpenSSH sshd 缓冲区错误漏洞(CVE-2016-10012)
OpenSSH sshd 安全漏洞(CVE-2016-10708)
OpenSSH PAM启用验证延迟信息泄露漏洞(CVE-2003-0190)
OpenSSH SCP客户端文件破坏漏洞(CVE-2004-0175)
OpenSSH enables AllowTcpForwarding 安全漏洞(CVE-2004-1653)
OpenSSH LoginGraceTime远程拒绝服务漏洞(CVE-2004-2069)
OpenSSH GSSAPI 证书信息泄露漏洞(CVE-2005-2798)
OpenSSH GSSAPI认证终止信息泄露漏洞(CVE-2006-5052)
OpenSSH S/Key 远程信息泄露漏洞(CVE-2007-2243)
OpenSSH glob表达式拒绝服务漏洞(CVE-2010-4755)
OpenSSH 远程拒绝服务漏洞(CVE-2010-5107)
OpenSSH 权限许可和访问控制问题漏洞(CVE-2014-2532)
OpenSSH'verify_host_key'函数输入验证错误漏洞(CVE-2014-2653)
OpenSSH'x11_open_helper()'函数权限许可和访问控制问题漏洞(CVE-2015-5352)
OpenSSH sshd monitor.c文件权限许可和访问控制问题漏洞(CVE-2015-6564)
OpenSSH sshd 安全漏洞(CVE-2016-10011)
OpenSSH sshd CRLF注入漏洞(CVE-2016-3115)
OpenSSH 信息泄露漏洞(CVE-2016-6210)
OpenBSD OpenBSD OpenSSH 信任管理问题漏洞(CVE-2005-2666)
OpenSSH X11UseLocalhost X11转发会话劫持漏洞(CVE-2008-3259)
OpenSSH 信息泄露漏洞(CVE-2011-4327)
OpenSSH数字错误漏洞(CVE-2011-5000)
OpenSSH auth_parse_options函数信任管理问题漏洞(CVE-2012-0814)
OpenSSH sshd monitor组件输入验证错误漏洞(CVE-2015-6563)
服务器加密通信支持的SSL加密算法（原理扫描）
服务器支持的SSL加密协议（原理扫描）
ICMP时间戳检测(原理扫描)
SSH版本信息可被获取(原理扫描)
SSH协议支持的算法(原理扫描)
未知服务端口可能会被特洛伊木马感染

漏洞解决方案

在E1709P08版本之前，openssh的版本号都是H3C，如果漏扫设备是基于openssh版本号来判断是否存在漏洞，那就是误报。

在E1709P08以及更新的版本，openssh版本号为openssh版本是8.9，现场可以升级版本之后再扫描