CSAP-S是否涉及CVE-2016-20012 CVE-2021-41617 OpenSSH 安全漏洞

漏洞相关 **杨雅伦** 2022-05-13 发表

漏洞相关信息

漏洞编号： CVE-2016-20012 CVE-2021-41617
漏洞名称： OpenSSH 安全漏洞
产品型号及版本： csap-s

漏洞描述

CVE-2016-20012 CVE-2021-41617 OpenSSH 安全漏洞
一、漏洞详情

OpenSSH是SSH（Secure SHell）协议的免费开源实现。

OpenSSH项目发布了OpenSSH 8.8安全更新，修复了OpenSSH 6.2 到 8.7版本中的 sshd(8)中的一个权限提升漏洞（CVE-2021-41617）。

当sshd(8)在执行AuthorizedKeysCommand或AuthorizedPrincipalsCommand时，未能正确地初始化，其中AuthorizedKeysCommandUser或AuthorizedPrincipalsCommandUser指令被设置为以非root用户身份运行。相反，这些命令将继承 sshd(8) 启动时的组的权限，根据系统配置的不同，继承的组可能会让辅助程序获得意外的权限，导致权限提升。在sshd_config(5)中，AuthorizedKeysCommand和AuthorizedPrincipalsCommand都没有被默认启用。

建议受影响用户做好资产自查以及预防工作，以免遭受黑客攻击。

二、影响范围

OpenSSH版本6.2-8.7

漏洞解决方案

升级到E1145P01，openssh版本已经升级到8.8,低版本的漏洞不涉及