关于CAS涉及虚机内核逃逸漏洞CVE-2019-14835问题的技术公告

陈明槐 2019-10-24 发表

问题描述

【涉及版本】

CAS1.0、CAS2.0、CAS3.0

CAS 5.0 E0535之前版本（不含E0535）

【问题描述】

CAS是基于QEMU-KVM实现的虚拟化平台，涉及QEMU-KVM虚机内核逃逸漏洞（CNVD-C-2019-135439，对应CVE-2019-14835）。攻击者利用该漏洞，可在未授权的情况下实现虚机逃逸。

原因分析

无

规避措施/解决方案

方式一：

1、CAS1.0、至CAS3.0 E0306（不含）的版本：先至少升级至E0306版本，然后打vhost.ko漏洞修复补丁（vhost_update.tar.gz）

2、CAS3.0 E0306（含）至CAS5.0 E0535（不含）的版本：打vhost.ko漏洞修复补丁（vhost_update.tar.gz）

漏洞修复补丁的操作方法请参考漏洞补丁版本E0530L15下的《H3C CAS QEMU-KVM虚拟机内核逃逸漏洞（CVE-2019-14835）修复补丁使用指导V1.00》

方式二：

升级至E0535以及后续版本