2016 年 9 月 6 日，星期二

漏洞聚焦：Kaspersky 未处理的 Windows 邮件拒绝服务漏洞

漏洞发现者：思科 Talos 团队的“冰壁”Marcin Noga。

概述

Talos 宣布在 Kaspersky Anti-Virus 中发现了一个本地拒绝服务漏洞 TALOS-2016-0175/CVE-2016-4329。系统用户可以通过在系统中执行恶意代码，引发对 Kaspersky avpui.exe 进程的拒绝服务攻击。因此，受 Kaspersky 自我保护功能保护的 avpui.exe 进程就会停止运行。

只有已经进入系统的用户，才可以利用此漏洞。然而，此漏洞也可能会被恶意用户利用，他们希望致使防病毒扫描功能停止向其他用户通知关于潜在恶意活动的信息。这可能构成一系列危害期延长的恶意活动中的一环。管理员应确保安装最新版本的 Kaspersky 软件以消除此漏洞。

覆盖

以下 Snort 规则将会检测出漏洞攻击尝试。请注意，Talos 未来可能会发布更多规则，当前规则会根据未来得到的更多漏洞信息而有所变更。如需获取有关最新规则的信息，请参阅防御中心或 Snort.org。

Snort 规则：39918、39919

发布者：Martin Lee 发布时间：上午 11:03
标签：零日、CVE-2016-4329、Kaspersky、漏洞聚焦