2016 年 8 月 26 日，星期五

漏洞聚焦：卡巴斯基互联网安全套装中存在内核信息泄漏漏洞和多个 DOS 问题

漏洞发现者：思科 Talos 团队的 Piotr Bania 和“Icewall”Marcin Noga。

概述

Talos 在卡巴斯基 (Kaspersky) 的互联网安全产品中发现了多个漏洞，攻击者可以利用这些漏洞发起本地拒绝服务攻击，或者在任何运行卡巴斯基互联网安全软件的计算机上造成内存泄漏。

详细信息

为了提供防病毒功能，卡巴斯基软件会通过名为 KLIF 的驱动程序挂接到 Windows API。Talos 发现，该驱动程序处理被拦截的 *NtUserCreateWindowEx* 和 *NtAdjustTokenPrivileges* 调用的方式存在两个漏洞。这两个漏洞都能导致攻击者在安装了卡巴斯基 KLIF 驱动程序的计算机上运行恶意应用，利用无效参数执行恶意 API 调用。这会导致驱动程序尝试访问无法访问的内存，从而引发系统崩溃。

通过卡巴斯基的 KL1 驱动程序，攻击者还可以进一步发起本地拒绝服务攻击。恶意用户可以向 KL1 驱动程序发送经特殊设计的 IOCTL 调用。在特定条件下，这会导致驱动程序读取已分配缓存以外的内存，有可能引发内存访问违例，从而造成系统崩溃。

在某些情况下，攻击者可以利用经特殊设计的 IOCTL 调用，通过在 kldisk.sys 驱动程序中无效实施 KlDiskCtl 服务，将内核内存内容泄漏到用户空间 (userland)。攻击者可能会利用这种方式从内核地址空间获取与安全性相关的信息，并结合使用其他漏洞攻击本地系统，例如破坏*地址空间布局随机化* (ASLR) 等安全功能。

这些漏洞所影响的软件包括 Kaspersky Internet Security 16.0.0（KLIF 驱动程序版本 10.0.0.1532），但是也有可能影响该软件的其他版本。由于在任何系统中，防病毒软件都是以底层权限运行的，所以此类软件中的漏洞很可能会备受攻击者关注。虽然这两个漏洞并不

十分严重，但是管理员应意识到安全系统本身也可能会被威胁发起者用作攻击媒介，所以坚持为安全系统安装所有补丁至关重要。

有关更多信息，请参阅下列漏洞报告：

- TALOS-2016-0166 / CVE-2016-4304
- TALOS-2016-0167 / CVE-2016-4305
- TALOS-2016-0168 / CVE-2016-4306
- TALOS-2016-0169 / CVE-2016-4307

本着以负责任的态度进行披露的宗旨，我们在发现这些漏洞后立即通知了卡巴斯基。在确认了卡巴斯基已发布相应的补丁来修复这些漏洞后，我们才公开了上述信息。

覆盖

以下 Snort 规则可以检测相关的漏洞攻击活动。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：39047-39048、39078-39079、38849-38850

发布者：Holger Unterbrink；发布时间：10:54
标签：CEV-2016-4306、CVE-2016-4304、CVE-2016-4305、CVE-2016-4307、卡巴斯基、漏洞聚焦