2016 年 12 月 14 日，星期三

漏洞聚焦：NVIDIA Windows 内核模式驱动程序中的本地拒绝服务漏洞已修复

在复杂系统和软件中，漏洞无可避免。操作系统和设备驱动程序是抽象层帮助隐藏复杂性并允许硬件和软件通信的主要示例。因此，如果发现可能危害、中断或使系统停止的漏洞，必须小心修复它们。Talos 与 NVIDIA 共同披露了 NVIDIA Windows 内核模式驱动程序中存在的本地拒绝服务漏洞：TALOS-2016-0217 (CVE-2016-8823)。

TALOS-2016-0217 表现为 NVIDIA Windows 内核模式驱动程序的通信功能中，消息处理存在缺陷。攻击者利用此缺陷，可能会导致拒绝服务情况，使系统进入漏洞检查状态（蓝屏崩溃）。运行向驱动程序发送经特殊设计的消息的应用可能会触发此漏洞。

已知受影响版本：

- NVIDIA GeForce Windows 内核模式驱动程序 372.70 (21.21.13.7270)
- NVIDIA GeForce Windows 内核模式驱动程序 372.90 (21.21.13.7290)

有关此漏洞的更多详细信息，请访问我们网站上的“漏洞咨询”门户，网址为：

http://www.talosintelligence.com/vulnerability-reports/

为了响应此次漏洞公告，NVIDIA 发布了软件更新（版本 376.33，可下载），以解决此缺陷。此外，Talos 还制定了 Snort 规则，用于检测尝试利用此漏洞的行为。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：40934-40935

发布者：ALEXANDER CHIU；发布时间：13:00

标签：拒绝服务、NVIDIA、补丁、SNORT 规则、漏洞