2016 年 7 月 11 日，星期一

漏洞聚焦：Intel HD Graphics Windows 内核驱动程序本地代码执行漏洞

漏洞发现者：Piotr Bania。

近日，Talos 与 Intel 共同披露了所发现的 TALOS-2016-0087。这是 Intel HD Graphics Windows 内核驱动程序中的一个本地任意代码执行漏洞。此漏洞存在于该驱动程序的通信功能中。攻击者可以通过向该驱动程序发送经特殊设计的消息来利用这一漏洞，从而导致拒绝服务或任意代码执行。需要注意的是，只有在本地环境中才能利用此漏洞。本着负责任的态度，我们已通过漏洞报告和披露指南，向 Intel 披露了这一漏洞。

TALOS-2016-0087 详情

TALOS-2016-0087 (CVE-2016-5647) 是 Intel HD Graphics Kernel Mode Driver for Windows 中的一个任意代码执行漏洞。攻击者可以通过向 Intel HD Graphics 驱动程序发送经特殊设计的 D3DKMTEscape 请求来触发此漏洞，从而导致空指针解引用。攻击者可以利用此漏洞来实现拒绝服务攻击，或者在受影响的系统中执行任意代码。此漏洞攻击只能在本地环境下实现，例如，需要用户执行专为利用受 TALOS-2016-0087 影响的系统而设计的二进制文件。

此漏洞的严重性视攻击者试图攻击的系统而定。在运行 Windows 7 或更早版本的系统上，利用此漏洞可导致在系统环境中执行任意代码；在运行 Windows 8 或更高版本的系统上，利用此漏洞很可能导致系统崩溃（拒绝服务）。

为了实现任意代码执行，攻击者需要具备在 Windows 中分配或映射空页面的能力。当内核空间出现空指针解引用时，已引起环境切换的用户模式应用仍会以较低的内存保留映射关系。攻击者可以利用这一点映射空页面，然后触发漏洞以控制解引用的内容。在这种情况下，用户控制的值可能是一个函数指针，并能导致任意代码执行。

在运行 Windows 7 及更早版本的系统上，可以通过使用 NTVDM（NT 虚拟 DOS 机）子系统来分配或映射空页面。但是，在 Windows 8 和更高版本的系统上，为了预防此类攻击，此功能已被移除。此外，运行 32 位 Windows 8 或更高版本的系统默认禁用 NTVDM，必须在控制面板中手动重新启用。运行 64 位 Windows 的系统中没有 NTVDM 子系统。请注意，这些

预防措施并非万无一失。例如，攻击者可能通过操纵另一个驱动程序来将用户控制的数据引向空页面，不过这种情况并不像上述用户模式映射那样常见。

有关此漏洞的完整技术详情，请点击此处查看我们网站上的漏洞公告。

结论

虽然向后兼容性让无法立即升级的用户和组织获益良多，但是同时也带来了潜在的安全风险。网络攻击者非常清楚，很多组织为了满足旧版应用的要求而无法升级到新版操作系统。因此，要抵御利用旧版功能发动的攻击，就需要采取其他预防攻击的方法。请确保您的操作系统安装了最新的安全更新，并安装相应的驱动程序。此外，使用反恶意软件的软件也有助于预防这类风险。

Talos 将继续按部就班地调查和识别第三方库与软件包中的零日漏洞，以便为保护我们的客户和整个互联网社区贡献力量。

以下 Snort 规则可帮助检测和预防试图利用 TALOS-2016-0087 发起的攻击：

37519-37520

发布者：Earl Carter；发布时间：下午 12:19
标签：漏洞、漏洞聚焦