2016 年 6 月 28 日，星期二

漏洞聚焦：LIBREOFFICE RTF 漏洞

漏洞发现者：思科 Talos 团队的 Aleksandar Nikolic。

Talos 宣布在 LibreOffice 的 RTF 解析器中发现了一个释放后使用漏洞 (CVE-2016-4324/TALOS-CAN-0126)。在解析同时包含样式表 (Stylesheet) 和上标 (Superscript) 令牌的文档时，便会出现此漏洞。通过对同时包含样式表和上标元素的 RTF 文档进行特殊设计，可以命令 LibreOffice 访问指向堆中以前使用的内存的无效指针。攻击者通过精心操纵堆中的内容，就可以利用漏洞来执行任意代码。利用此漏洞需要用户执行文件打开操作。

富文本格式 (RTF) 是一种专为文档交换而设计的跨平台文档格式。虽然从 2008 年起，该格式的标准不再更新，但是该格式在各种文字处理套件中仍然受到广泛的支持。过去，攻击者曾利用 MS Office 中的 RTF 解析器漏洞发起攻击，并将 RTF 文件作为嵌入其他恶意对象的载体。利用此类漏洞的攻击依赖于用户操作，也就是说，用户必须打开文件，才会触发攻击。提高用户对此类漏洞的警惕性有助于提醒人们不要打开未知或可疑的电子邮件或文件。尽管目前我们尚未发现任何此漏洞正在被大规模利用的迹象。但是，我们仍然建议管理员将 LibreOffice 系统更新到最新版本，以便消除此漏洞。

Snort 规则：39148、39149

发布者：MARTIN LEE；发布时间：15:01