2016 年 8 月 15 日，星期一

漏洞聚焦：Lexmark Perceptive 文档过滤器中存在多个远程代码执行漏洞

漏洞发现者：思科 Talos 团队的 Tyler Bohan 和 Marcin Noga。

Talos 今天发布了三个在 Lexmark Perceptive 文档过滤器库中发现的新漏洞：TALOS-2016-0172、TALOS-2016-0173 和 TALOS-2016-0183。利用经特殊设计的文件，这些漏洞可被用于执行远程代码。

概述

这三个漏洞存在于 Lexmark 文档过滤器的解析引擎中，eDiscovery、DLP、大数据和内容管理等诸多服务都使用了该解析引擎。这些服务普遍使用 Lexmark 文档过滤器库来深入检测各种文件格式，以提供格式转换功能（例如将 Microsoft 文档格式转换为其他格式）。Lexmark 开发这个产品是为了与其他具有相同功能的第三方库和开源库进行竞争。

对许多企业来说，文档转换是一个重要的功能，因为他们会尝试将非结构化数据解决方案转换为更适合工作的结构化数据解决方案来提高业务效率。

本次发布的三个漏洞可以使攻击者以经特殊设计的文件（XLS、Bzip2 和复合二进制文件格式 [MS-CFB]）为媒介，实现远程代码执行。成功利用这些漏洞的攻击者将能够在用户环境中执行远程代码，并有可能获得对受攻击资源的完全控制权限。

如需了解 Perceptive 文档过滤器的详细信息，请点击此处访问 Lexmark 网站。

详细信息

TALOS-2016-172

此漏洞存在于 XLS 文档的解析和转换过程中。利用此越界写入漏洞，攻击者可以制作经特殊设计的 XLS 文件，来达到远程代码执行目的。攻击者可以通过网络钓鱼方式，将经特殊设计的 XLS 文件作为文档附件发送给用户，或者通过 URL 将用户定向到文件所在的位置下载执行。

点击此处可获得完整的技术建议。

TALOS-2016-0173

此漏洞存在于 bzip2 文档的解析和转换过程中。bzip2 是受开源平台广泛支持的高压缩文件格式。通过使用经特殊设计的 bzip2 文件，攻击者可以引发越界写入，从而在受害者的计算机上远程执行任意代码。

点击此处可获得完整的技术建议。

TALOS-2016-0183

此漏洞存在于复合二进制文件格式 (MS-CFB) 的处理过程中。MS-CFB 是 Microsoft 提供的一种文件类型，可以在文件内建立类似于文件系统的结构，以便能够存储任意数据流和特定应用数据流。通过使用经特殊设计的文件，攻击者可以利用堆溢出漏洞发动攻击。

点击此处可获得完整的技术建议。

覆盖

为了检测上述漏洞，Talos 发布了下列 Snort 规则：39868-39869、39871-39872

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、FireSIGHT 管理中心或 Snort.org。

如需获取更多有关零日攻击或漏洞的报告和信息，请访问：
http://talosintelligence.com/vulnerability-reports/

发布者：Martin Lee；发布时间：12:46