2017 年 8 月 28 日，星期一

漏洞聚焦：LexMark Perceptive 文档过滤器代码执行漏洞

概述

Talos 现披露两个 LexMark Perceptive 文档过滤器代码执行漏洞。Perceptive 文档过滤器是一组库，用于针对多种用途解析大量不同类型的文件格式。此前，Talos 已详细介绍过这些过滤器及其工作方式。如需获取解决这些漏洞的软件更新，请点击此处。

TALOS-2017-0322

漏洞发现者：思科 Talos 团队的 Marcin Noga

TALOS-2017-0322/CVE-2017-2821 是 LexMark Perceptive 文档过滤器的 PDF 解析功能中的一个代码执行漏洞。此特定漏洞属于与“GfxFont”变量有关的释放后使用类漏洞，可以通过经特殊设计的 PDF 文档触发，进而导致代码执行。有关该漏洞的完整详细信息，请点击此处。

TALOS-2017-0323

漏洞发现者：思科 Talos 团队的 Marcin Noga 和 Lillyth Wyatt

TALOS-2017-0323/CVE-2017-2822 是 LexMark Perceptive 文档过滤器的图像渲染功能中的一个代码执行漏洞。此特定漏洞可以通过经特殊设计的 PDF 文档触发，导致对已损坏的 DCTStream 的函数调用，最终导致用户控制的数据被写入堆栈中。有关该漏洞的完整详细信息，请点击此处。

防护

以下 Snort 规则可以检测相关的漏洞攻击尝试活动。请注意，Talos 将来可能会发布更多规则，当前规则会根据将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：42313-42314、42399-42400

发布者：NICK BIASINI 发布时间：11:30
标签：零日、TALOS、漏洞研究、漏洞聚焦