2017 年 5 月 16 日，星期二

发现并修复 MuPDF 中的任意代码执行漏洞

Talos 披露了 Artifex MuPDF 渲染器中存在的两个漏洞。MuPDF 是一个轻量级的 PDF 解析和渲染库，具有图片保真度高、速度快和代码精简等特点，这使之成为相当流行的 PDF 库，可嵌入到各种项目中，尤其是移动和 Web 应用。无论攻击者选择利用哪个漏洞，都会在目标设备上引发任意代码执行。这两个漏洞均已被负责任地披露，Artifex 也已发布软件更新来进行修复。

漏洞详细信息

Artifex MuPDF 渲染器中存在两个内存损坏漏洞，一旦被攻击者利用，可能会导致任意代码执行。出现这两个漏洞是因为对 PDF 文件某些部分的解析和处理不当。

- TALOS-2016-0242 - MuPDF Fitz 库字体字形缩放代码执行漏洞
  这是一个堆越界写入漏洞，当必须按比例缩小字体字形时，它会出现在字形缩放代码中。

  漏洞发现者：Aleksandar Nikolic。

- TALOS-2016-0243 - MuPDf JBIG2 解析器代码执行漏洞
  这是一个基于堆的缓冲区溢出漏洞，出现在针对 PDF 中嵌入的 JBIG2 图像的 JBIG2 图像解析功能中。

  漏洞发现者：Aleksandar Nikolic 和 Cory Duplantis。

如果攻击者专门制作一个 PDF 文件，并让受害者使用 MuPDF 打开该 PDF 文件，就可以利用这两个漏洞。在基于邮件的攻击场景中，如果用户打开恶意 PDF 附件，或者从托管用户内容的站点中下载恶意 PDF，攻击者就可以实现远程代码执行。

有关这两个漏洞的完整技术详细信息，请参阅我们网站上发布的漏洞公告：

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

防护

以下 Snort 规则可检测试图利用这些 MuPDF 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漏洞信息而有所变更。如需获取有关最新规则的所有信息，请参阅 Firepower 管理中心或 Snort.org。

Snort 规则：41470-41471、41224-41225

发布者：ALEXANDER CHIU；发布时间：0:47
标签：MUPDF、SNORT 规则、漏洞研究