2017 年 7 月 7 日，星期五

漏洞聚焦：TALOS-2017-0311、0319 和 0321 - Poppler PDF 库中存在多个远程代码执行漏洞

该漏洞由思科 Talos 团队的 Marcin Noga、Lilith Wyatt 和 Aleksandar Nikolic 发现。

概述

Talos 团队在 freedesktop.org Poppler PDF 库中发现了多个漏洞。攻击者可以利用这些漏洞完全控制受害者的计算机。如果攻击者构建经特殊设计的 PDF 文件并且受害者打开此文档，攻击者代码将以本地用户权限得到执行。

详细信息

Poppler 是用于显示 PDF 文件的共享库，用作不同企业和开源解决方案（例如，Gimp）内的中间件。Poppler 分离自 XPDF，是 PDF ISO 标准的完整实现。Talos 团队在 Poppler 库中发现三个远程代码执行漏洞。

TALOS-2017-0311 / CVE-2017-2814 - Poppler PDF 图形显示 DCTStream::readScan() 代码执行漏洞

图形在渲染 Poppler-0.53.0 功能时存在可利用的堆溢出漏洞。经特殊设计的 PDF 会导致图片在发生分配后调整大小，导致 DCTStream::readScan() 功能中的堆溢出被触发。这可能会导致攻击者使用本地用户权限发动代码执行。

TALOS-2017-0319 / CVE-2017-2818 - Poppler PDF 图形显示 DCTStream::readProgressiveSOF() 代码执行漏洞

Talos 发现图形在渲染 Poppler-0.53.0 功能时存在可利用的堆溢出漏洞。经特殊设计的 PDF 可在图像渲染过程中导致颜色组件数量过大，从而引起堆损坏。攻击者可以利用此漏洞设计 PDF 文件，进而以本地用户权限在受害者的计算机上执行恶意代码。

这个漏洞以前曾被发现过 (CVE-2005-3627)，后来 DCTStream::readBaselineSOF 得到修订，但是遗漏了 readProgressiveSOF 功能中的漏洞。

TALOS-2017-0321 / CVE-2017-2820 - Poppler PDF 库 JPEG2000 级代码执行漏洞

Talos 团队发现 JPEG 2000 图形在解析 Poppler 0.53.0 库的功能时存在可利用的整数溢出漏洞。攻击者可以构建经特殊设计的 PDF 文件，进而使用此漏洞触发整数溢出。在后面的代码执行流程中，该漏洞会导致堆上的内存被覆盖，使得攻击者可能会利用本地用户权限发送任意代码执行。跟前面提到的另外两个漏洞一样，受害者必须在使用此库的应用中打开恶意 PDF，攻击者才能利用此漏洞。随最新版的 Ubuntu Linux 一起提供的默认 PDF 阅读器 Evince 就是一个易受攻击的应用示例。

补充说明

我们要强调一点，TALOS-2017-0311 和 TALOS-2017-0321 位于 Poppler 内部，所以请不要使用无人维护的 JPEG 和 JPEG2000 解码器。即使是 Poppler 的文档，也强烈建议您不要使用此类解码器。强烈建议您使用更强大和更新的外部实施（如 libjpeg 和 openjpeg）来构建 Poppler 库。但是，默认情况下，Ubuntu 不会为 JPEG2000 执行此操作，而是使用无人维护的代码，从而导致 Ubuntu 编译的版本容易受到这些问题的攻击。

Talos 看到利用恶意 PDF 文件的客户端攻击每天都在发生。如果贵公司正在使用基于 Popper 的应用，那么攻击者可能会针对该应用利用其中一个漏洞发动攻击。这表明除了操作系统，保持其他所有应用为最新有多么重要。

有关更多技术详情，请参阅下列 Talos 漏洞报告：
TALOS-2017-0311
TALOS-2017-0319
TALOS-2017-0321

防护

以下 Snort 规则可以检测此漏洞的漏洞攻击活动。请注意，Talos 未来可能会发布更多规则，当前的规则可能会根据可能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 FireSIGHT 管理中心或 Snort.org

Snort 规则：42273-42274、42319 - 42320 和 42352-42353

发布者：HOLGER UNTERBRINK；发布时间：11:27