2017 年 10 月 26 日，星期四

漏洞聚焦：Apache OpenOffice 漏洞

漏洞发现者：思科 Talos 团队的“冰壁”Marcin Noga

一般信息

今天，Talos 发布在 Apache OpenOffice 应用中发现的以下三个新漏洞的详细信息：第一个漏洞 TALOS-2017-0295，是在 OpenOffice Writer 中发现的；第二个漏洞 TALOS-2017-0300，是在 Draw 应用中发现的；第三个漏洞 TALOS-2017-0301，是在 Writer 应用中发现的。所有三个漏洞都允许执行任意代码。

TALOS-2017-0295 - Apache OpenOffice DOC WW8Fonts 构造函数中的 Apache OpenOffice 远程代码执行漏洞 (CVE-2017-9806)

该漏洞存在于 OpenOffice 文字处理应用的 WW8Fonts::WW8Fonts 类中。攻击者可以使用特殊设计的恶意字体构建恶意 .doc（Microsoft Word 二进制文件格式）文件。如果 WW8Fonts::WW8Fonts 类构造函数解析该字体，就会导致越界写入漏洞，进而导致远程代码执行。

有关更多技术详情，请参阅相应 Talos 漏洞报告。
另请参阅 OpenOffice 公告。

已知存在漏洞的版本

Apache OpenOffice 4.1.3

TALOS-2017-0300 - Apache OpenOffice PPT PPTStyleSheet 级别代码执行漏洞 (CVE-2017-12607)

Apache OpenOffice 的“PPTStyleSheet:PPTStyleSheet”函数中存在一个可利用的越界写入漏洞。此组件是用于创建幻灯片演示文稿的 Draw 应用的一部分。攻击者可以创建特殊设计的 PPT 文件来利用此漏洞，造成越界写入，并且在当前用户环境中在受害者的计算机本地执行任意代码。

有关更多技术详情，请参阅相应 Talos 漏洞报告。
另请参阅 OpenOffice 公告。

已知存在漏洞的版本

Apache OpenOffice 4.1.3

TALOS-2017-0301 - Apache OpenOffice DOC ImportOldFormatStyles 代码执行漏洞 (CVE-2017-12608)

在 Apache OpenOffice 4.1.3 中（更具体地说是在其用于创建文档的 Write 应用中），“WW8RStyle::ImportOldFormatStyles”函数存在一个可利用的越界写入漏洞。攻击者可以使用特殊设计的 doc 文件造成越界写入，从而在当前运行的用户环境中在受害者计算机本地执行任意代码。

有关更多技术详情，请参阅相应 Talos 漏洞报告。
另请参阅 OpenOffice 公告。

已知存在漏洞的版本

Apache OpenOffice 4.1.3

讨论

Apache OpenOffice 是一款常用的免费开源办公软件，可以替代其他 Office 套件产品。Office 套件软件（例如文字处理器）中的漏洞对攻击者进行客户端攻击非常有用。攻击者经常通过电子邮件附件发送利用这些漏洞的恶意文档，在运用某些社交工程手段诱使受害者打开文档之后，执行恶意命令。OpenOffice 并非唯一一款存在此类问题的产品，之前 Talos 在其他文字处理应用和库中（例如 LibreOffice，甚至包括 Windows 内核的字体驱动程序）也发现了类似漏洞。

我们已经监测了很多起利用此攻击媒介发起的有针对性攻击活动。我们最近分析的针对韩国用户的攻击就是一个很好的例子。攻击者利用 Hangul Word Processor (HWP) 中的一个漏洞感染了受害者的计算机。这表明用户必须及时更新所有应用，而不仅是更新操作系统。如果您是一名 OpenOffice 用户，我们强烈建议您尽早安装必要的更新。

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 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 FireSIGHT 管理中心或 Snort.org

Snort 规则：42008 - 42009、42144 - 42145、42076 - 42077。

发布者：HOLGER UNTERBRINK；发布时间：上午 10:26
标签：APACHE、CVE-2017-12607、CVE-2017-12608、CVE-2017-9806、OPENOFFICE、漏洞、漏洞聚焦