2016 年 10 月 25 日，星期二

漏洞聚焦：LibTIFF 问题导致代码执行

漏洞发现者：思科 Talos 团队的 Tyler Bohan。

Talos 发布了在 LibTIFF 库中发现的多个漏洞（TALOS-2016-0187、TALOS-2016-0190 和 TALOS-2016-0205）。第一个漏洞 (TALOS-2016-0187) 是可被利用的基于堆的缓冲区溢出漏洞，会对 LibTIFF TIFF2PDF 转换工具产生影响。第二个漏洞 (TALOS-2016-0190) 会影响 TIFF 图像的解析和处理，并且最终会导致远程代码执行。最后一个漏洞 (TALOS-2016-0205) 是可被利用的基于堆的缓冲区溢出漏洞，在使用 LibTIFF 的 PixarLogDecode API 处理压缩 TIFF 图像时出现。通过诱骗用户处理异常 TIFF 文档，攻击者可以使用其中任何一个漏洞在受攻击的系统上实现远程代码执行。

标记图像文件格式 (TIFF) 是 20 世纪 80 年代开发的一种通用文件格式，其目的是让迅速发展的图形处理行业能以无损格式存储图像数据。从那时起，TIFF 文件就在印艺行业和电子传真系统中得到广泛采用。

LibTIFF 是免费分发的软件库。基于 Windows 和 UNIX 的平台（包括 Linux 和 MacOS X）均支持 LibTIFF。利用 LibTIFF，系统能够读取、写入和处理 TIFF 格式的文件。TIFF 文件格式的优势之一在于其可扩展性。该格式引入了许多标记，用于代表与文件中包含的数据相关的特定信息。一些标记由 TIFF 标准定义，并且必须由该文件格式的解释器提供支持；另一些标记则是后续追加定义的，这些标记的受支持和可识别程度各不相同。

CVE-2016-5652 (TALOS-2016-0187) - LibTIFF tiff2pdf JPEG 压缩表堆缓冲区溢出
CVE-2016-8331 (TALOS-2016-0190) - LibTIFF FAX IFD 条目解析类型混淆
CVE-2016-5875 (TALOS-2016-0205) - LibTIFF PixarLogDecode 堆缓冲区溢出

详细信息

CVE-2016-8331 在使用标准版本中的 LibTIFF API 解析和处理 TIFF 图像期间出现。RFC 2306 定义了 TIFF 格式中使用的一系列字段，专用于受 LibTIFF 库全面支持的传真系统。该漏洞存在于处理“BadFaxLines”字段的过程中，可能会导致写入越界内存。攻击者可以通过精心制作的 TIFF 文件利用此漏洞，实现在受影响系统上执行任意代码的目的。

截至本文章发布，仍无针对 CVE-2016-8331 的补丁发布

CVE-2016-5875（由 Mathias Svensson 发现）在使用 LibTIFF 的 PixarLogDecode API 处理压缩 TIFF 图像时出现。要解压缩 TIFF 图像中的 PixarLog 压缩数据，LibTIFF 需要使用 Zlib 压缩库。首先，系统通过一个调用“PixarLogSetupDecode”的函数建立一个缓冲区。该缓冲区中包含需要传递给 Zlib 的参数。然后，系统在调用真正负责解压缩任务的 Zlib 库“解压缩”函数时，会使用此缓冲区。如果将过小的缓冲区传递给 Zlib“解压缩”函数，会造成堆溢出。这可能会被利用实现远程代码执行。

最后一个漏洞 (CVE-2016-5652) 存在于与 LibTIFF 捆绑的 Tiff2PDF 工具中，在 TIFF 文件使用 JPEG 压缩时出现。默认情况下，此工具会在标准构建过程中安装。

TIFF 为图像自身的多种压缩算法提供支持。JPEG 压缩就是这样一种算法。此漏洞在计算图像图块大小时出现。攻击者精心设计的 TIFF 图像文件能引发越界写入，最终实现远程代码执行。通过使用精心设计的 TIFF 文档诱骗用户使用此实用程序，攻击者可以引发基于堆的缓冲区溢出，从而实现远程执行代码的目的。

测试版本

LibTiff - 4.0.6

防护

尚无解决这些问题的官方 LibTIFF 版本。您可以从 CVS 存储库获取 CVE-2016-5652 和 CVE-2016-5875 的补丁（目前尚未发布针对 CVE-2016 8331 的补丁）。为了保护我们的客户，Talos 已经发布了相关规则来检测利用这些漏洞的攻击尝试。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，请参阅防御中心或 Snort.org。

Snort 规则：40525-40526、40533-40538 和 40539-40540

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：EARL CARTER；发布时间：11:47
标签：零日、LIBTIFF、 漏洞