2016 年 7 月 19 日，星期二

漏洞聚焦：Apple 图像文件处理远程代码执行漏洞

漏洞发现者：思科 Talos 团队的 Tyler Bohan。

在各种各样的文件格式中，有许多是专为特定行业的专门用途而设计的。Apple 提供多种 API 作为接口，专用于访问 Apple OS X 平台上多种图像格式的图像数据。Talos 披露了 Apple OS X 中存在的与处理图像格式相关的五个远程代码执行漏洞：TALOS-2016-0171、TALOS-2016-0180、TALOS-2016-0181、TALOS-2016-0183、TALOS-2016-186。

TALOS-2016-0171

标记图像文件格式 (TIFF) (CVE-2016-4631)

标记图像文件格式 (TIFF) 是平面设计师、摄影师和出版业普遍使用的文件格式，因为它能够以无损格式存储图像。TIFF 诞生于 20 世纪 80 年代中期，目的是建立一种通用的扫描图像文件格式。思科 Talos 团队发现，Apple 图像 I/O API 解析和处理平铺 TIFF 图像文件的方式存在漏洞。使用图像 I/O API 的应用在渲染经特殊设计的 TIFF 图像文件时，可能会造成基于堆的缓冲区溢出，最终导致攻击者能够在存在漏洞的系统和设备中执行远程代码。

此漏洞非常值得担忧，因为任何使用 Apple 图像 I/O API 的应用在渲染平铺 TIFF 图像时都可能会触发此漏洞。这意味着攻击者可以使用广泛的潜在攻击媒介（包括 iMessage、恶意网页、MMS 消息，或需要通过任何使用 Apple 图像 I/O API 的应用来渲染的其他恶意文件附件）传递成功利用该漏洞的负载。

此外，根据攻击者选择的传递方式，此漏洞还有可能以无需显式用户交互的方法利用，因为许多应用（例如 iMessage）会试图自动渲染以默认配置接收的图像。由于此漏洞同时存在于 OS X 10.11.5 和 iOS 9.3.2 中（相信所有更早的版本中也存在此漏洞），所以受其影响的设备数量十分惊人。

TALOS-2016-0180 和 TALOS-2016-0181

OpenEXR 文件格式（CVE-2016-4629 和 CVE-2016-4630）

OpenEXR 是一种高动态范围图像文件格式。该格式由工业光魔公司专为视觉特效行业而开发，目前广泛用于专业计算机图形中。该格式为以像素存储的信息的位深度提供了非常大的灵活性。但是，攻击者可以通过创建恶意 OpenEXR 文件来滥用这种灵活性，导致 Apple 图像 I/O 将图像中包含的信息写入预期的目标缓冲区以外的内存。

此外，图像 I/O 在处理 OpenEXR 文件中的 B44 压缩数据时存在漏洞。EXR 文件中压缩数据的大小是指定的。如果该值大于可以存储在 int 值中的数值，超出的用户数据会被写入预期空间以外的内存。

通过操控内存中的内容来建立必要的设置，攻击者可以利用这两个漏洞在设备上引发远程代码执行。

TALOS-2016-0183

数字资产交换文件格式 (CVE-2016-1850)

数字资产交换文件格式（也称为协同设计活动文件）是一种 XML 文件格式，用于在使用互不兼容的文件格式的数字内容创建工具之间交换文件。Apple Scene Kit 便是一种用于支持数字资产交换文件的 3D 建模框架。

利用此漏洞，攻击者可通过将经特殊设计的数字资产交换文件传送到 Scene Kit，导致此框架将一种类型的对象作为另一种类型加以访问。在这种情况下，攻击者将有可能对错误类型的对象执行内存访问越界操作。因此，利用此漏洞可在设备上引发远程代码执行。

注：TALOS-2016-0183 在 OSX 10.11.5 中进行了修复。

TALOS-2016-0186

BMP 文件格式 (CVE-2016-4637)

BMP 文件格式由来已久，而且结构相当简单。BMP 文件报头包含与图像大小、布局和类型相关的信息。Apple 系统中处理图像高度属性的方法存在漏洞。如果用户在保存经特殊设计的 BMP 图像文件后将其打开，而该文件的部分大小信息经过操纵，则可能会受到漏洞攻击。此漏洞会导致写入越界，当在使用 Apple 核心图形 API 的任何应用中打开经特殊设计的 BMP 图像时，可能会引发远程代码执行。

已知存在漏洞的版本

TALOS-2016-0171

OS X Mavericks v10.9.5、OS X Yosemite v10.10.5、OSX El Capitan 10.11.5、iOS 9.3.2、watchOS 2.2.1 和 tvOS 9.2.1

TALOS-2016-0180 和 TALOS-2016-0181

OS X Mavericks v10.9.5、OS X Yosemite v10.10.5 和 OSX El Capitan 10.11.5

TALOS-2016-0183

OSX El Capitan 10.11.4

TALOS-2016-0186

OS X Mavericks v10.9.5、OS X Yosemite v10.10.5、OSX El Capitan 10.11.5、iOS 9.3.2、watchOS 2.2.1 和 tvOS 9.2.1

总结

图像文件是绝佳的攻击媒介，因为它们可以轻松通过 Web 内容或邮件分发，而不会引起收件人的怀疑。这些漏洞具有更高的危险性，因为 Apple OS X 平台上的软件广泛使用 Apple 核心图形 API、Scene Kit 和图像 I/O。

组织应安装最新的软件补丁，来杜绝这些漏洞。为保护我们的客户，Talos 推出了 Snort 规则来检测利用这些漏洞的攻击企图。此外，对于合法业务中永远不会或很少会碰到的文件类型，组织还应考虑由网络网关来阻止它们。

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、FireSIGHT 管理中心或 Snort.org。

Snort 规则：16222、39634-39635、39597-39632

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://talosintel.com/vulnerability-reports/

发布者：EARL CARTER；发布时间：17:42

标签：APPLE、远程代码执行、漏洞聚焦