2016 年 10 月 3 日，星期一

漏洞聚焦：FreeImage 库 XMP 图像处理代码执行漏洞

漏洞发现者：Yves Younan。

Talos 与 FreeImage 联合披露发现漏洞 TALOS-2016-0189/CVE-2016-5684。

概述

FreeImage 是一款广泛使用的软件，目前已有 100 多种免费和付费产品集成了该软件，包括多媒体软件、游戏、开发人员工具、PDF 生成器等等。FreeImage 使用的可扩展元数据平台 (XMP) 是由 Adobe 制作的一种允许实时管理元数据的常见文件格式。据 Adobe 称，XMP 文件格式允许用户“在内容创建流程中，在将元数据嵌入到文件本身”。集成此文件格式的 FreeImage 3.17.0 软件易于受 XMP 图像“每像素颜色数”值溢出漏洞的攻击。一般而言，当 FreeImage 3.17.0 打开的 XMP 文件的“每像素颜色数”的值足够大（即数值过大）时，在使用该值的函数中，后续代码将无法正确处理该值。这就好比是有一个容量 99 盎司的玻璃杯，现在您打开水龙头，要注入超过 100 盎司的水。水会溢出，流到您不希望水流到的地方。从技术角度来说，过大的值在代码执行期间无法得到正确验证，并且可能触发越界写入。这会导致任意内存覆盖，并成为远程代码执行的直接诱因。攻击者可能会利用此漏洞，通过邮件附件或即时消息向您发送精心设计的恶意图像文件。

由于集成了 FreeImage 的软件如此广泛，并且攻击者利用此漏洞相对容易，我们强烈建议使用此类软件的所有用户尽快为自己的平台安装补丁。您可以点击此处，在 FreeImage 网站上找到软件列表。

FreeImage 于 8 月 7 日在 CVS 中发布了此漏洞的补丁，但尚未发布软件的新版本。如果您使用 FreeImage，我们建议您更新至 CVS 版本，以避免此漏洞带来的风险。

有关此漏洞的完整技术详情，请点击此处查看我们网站上的漏洞公告。

防护

为了保护我们的客户，Talos 已经发布了相关规则来检测利用该漏洞的攻击尝试。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：39883 和 39884

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

发布者：Tazz；发布时间：12:32
标签：Adobe、FreeImage、漏洞、XMP