2016 年 9 月 30 日，星期五

漏洞聚焦：OpenJPEG JPEG2000 mcc 记录代码执行漏洞

漏洞发现者：思科 Talos 团队的 Aleksandar Nikolic

概述

Talos 发现由 OpenJPEG 库实现的 JPEG 2000 图像文件格式解析器中存在一个可被利用的越界漏洞 (TALOS-2016-0193/CVE-2016-8332)。JPEG 2000 文件格式常用于在 PDF 文档中嵌入图像。本文中讲的这个漏洞可能会引发越界堆写入，造成堆破坏，进而导致任意代码写入。Talos 本着负责任的态度，已经向库维护者告知此漏洞，以确保库维护者能够提供相关补丁。

如果用户打开的文件中包含攻击者利用此漏洞精心设计的 JPEG 2000 图像，就可能成为此漏洞的受害者。此漏洞有多种利用方式，例如发动邮件攻击（用户打开垃圾邮件/网络钓鱼邮件中的附件会造成感染），或者潜伏在托管内容中（用户从 Google 云端硬盘或 Dropbox 下载文件会造成感染）。

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：40314-40315

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：WILLIAM LARGENT；发布时间：20:17
标签：零日、CVE-2016-8332、JPEG 2000、TALOS-2016-0193、漏洞研究、漏洞聚焦