2016 年 12 月 6 日，星期二

漏洞聚焦：ImageMagick 转换 Tiff 越界写入

漏洞发现者：Tyler Bohan

概述

Talos 公开了在 ImageMagick 中发现的越界写入漏洞 TALOS-2016-0216/CVE-2016-8707。ImageMagick 是一个图片编辑软件程序，用户可以通过它编辑和处理各种类型的图像文件。此特定漏洞存在于 ImageMagick 附带的转换实用程序中。该实用程序用于解析图像及转换图像格式。当尝试压缩 Adobe Deflate 压缩的 Tiff 图像时，会出现此漏洞。程序为保存 Tiff 图像相关解压数据而创建的缓冲区不够大，无法容纳解压流。在满足特定条件的情况下这会导致越界写入受控，会被用于进行完整的远程代码执行。有关该漏洞的完整详细信息，请点击此处。

防护

以下 Snort 规则将会检测出漏洞攻击尝试。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：40914-40915

发布者：WILLIAM LARGENT；发布时间：14:09

标签：SNORT 规则、TALOS、VULNDEV、漏洞研究