2017 年 10 月 19 日，星期四

漏洞聚焦：Google PDFium 的 TIFF 代码执行漏洞

概述

Talos 披露在最高 60.0.3112.101 版本（含该版本）的 Google Chrome 所用 PDFium 的 TIFF 图像解码功能中发现了一种 Off-By-One 读写漏洞。Google Chrome 是当今使用最广泛的 Web 浏览器，攻击者可以使用特殊设计的 PDF 文件触发该漏洞，导致内存损坏，并且可能窃取信息并执行代码。Google Chrome 版本 62.0.3202.62 中已修复此问题。

TALOS-2017-0432

漏洞发现者：思科 Talos 团队的 Aleksandar Nikolic

Talos-2017-0432 / CVE-2017-5133 是一种 Off-By-One 读写漏洞，存在于 PDFium 的 TIFF 图像解码功能中。PDFium 是谷歌开发的开源 PDF 渲染器，用于 Chrome Web 浏览器、在线服务和其他独立应用。在负责解码压缩的 TIFF 图像流的代码中存在一种基于堆的缓冲区溢出。

该漏洞是负责解析数据像素的功能造成的。在解析进程中，该功能始终会从“dest_buffer”中读取 4 字节，即使缓冲区长度不足 4 字节。这可能导致在堆上出现 Off-By-One 读取，随即出现 Off-By-One 写入。但是，为了访问这个存在漏洞的代码，需要满足几个条件。结果造成的 Off-By-One 读写可能导致内存损坏、信息泄漏或代码执行。有关该漏洞的完整详细信息，请点击此处。

防护

以下 Snort 规则可以检测相关的漏洞攻击尝试活动。请注意，Talos 将来可能会发布更多规则，当前规则会根据将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，请访问 Firepower 管理中心或 Snort.org。

Snort 规则：44294-44295

发布者：EARL CARTER；发布时间：16:51

标签：PDF、TIFF、漏洞