2017 年 8 月 30 日，星期三

漏洞聚焦：多个 Gdk-Pixbuf 漏洞

概述

今天，Talos 披露了在 Gdk-Pixbuf 工具包中发现的两个远程代码执行漏洞。该工具包用于多个桌面应用，包括 Chromium、Firefox、GNOME 缩略图工具、VLC 和其他软件。攻击者可以利用此漏洞完全控制受害者的计算机。如果攻击者构建经特殊设计的 TIFF 或 JPEG 图像并且诱使受害者打开该图像，攻击者代码将以本地用户权限得以执行。

详细信息

TALOS-2017-0377 -- CVE-2017-2870

漏洞发现者：思科 Talos 团队的 Marcin Noga 和 GDK Security 的 Tobias Mueller（二人分别独立发现）。

Gdk-Pixbuf 2.36.6 工具包的 tiff_image_parse 功能中存在可利用的整数溢出漏洞。经特殊设计的 TIFF 文件引发的堆溢出可导致远程代码执行。该漏洞存在在 TIFF 解析器中，只有使用高优化标志“-O3”（已使用 clang 测试）对库进行编译才会触发。该工具包带有一些已在“tiff_image_parse”函数内部定义的“if 语句”。其目的是检查整数溢出。不幸的是，编译器进行优化时会移除这些检查。问题是编译器将这些语句识别为“未定义的行为”，并将其移除以达到优化目的。最后，缺乏适当的整数溢出检查将导致堆溢出，进而使攻击者可以执行任意代码。

TALOS-2017-0366 -- CVE-2017-2862

漏洞发现者：思科 Talos 团队的 Marcin Noga。

Gdk-Pixbuf 2.36.6 的 gdk_pixbuf__jpeg_image_load_increment 功能中存在可利用的堆溢出漏洞。经特殊设计的 JPEG 文件引发的堆溢出可导致远程代码执行。该漏洞存在在 JPEG 解析器中，以“gdk_pixbuf__jpeg_image_load_increment”函数中输出缓冲区的错误计算量为基础，随后会导致在 libjpeg “null_convert”函数内部的内容转换过程中发生堆溢出。

防护

以下 Snort 规则可以检测此漏洞的漏洞攻击活动。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 FireSIGHT 管理中心或 Snort.org。

Snort 规则：39607、39615、43214-43215

发布者：WILLIAM LARGENT；发布时间：15:06
标签：零日、CVE-2017-2862、CVE-2017-2870、GDK、PIXBUF、TALOS、漏洞研究、漏洞聚焦