2017 年 10 月 4 日，星期三

漏洞聚焦：Computerinsel Photoline 中的多个漏洞

漏洞发现者：思科 Talos 团队的 Piotr Bania。

今天，Talos 发布了有关 Computerinsel GmbH PhotoLine 图像处理软件中发现的多个漏洞的详细信息。PhotoLine 由 Computerinsel GmbH 开发，是一款成熟的光栅和矢量图形编辑器，适用于 Windows 和 Mac OS X，也可用于桌面排版。

TALOS-2017-0387 (CVE-2017-2880)。攻击者可以利用 TALOS-2017-0427 (CVE-2017-2920) 和 TALOS-2017-0458 (CVE-2017-12106) 创建经特殊设计的图像文件。当用户在 PhotoLine 图像处理软件中打开这些文件时，攻击者将能够在存在漏洞的系统中远程执行任意代码。

技术详情

TALOS-2017-0387

攻击者可以通过操纵 GIF 内容来控制用于控制内存写入的计数器变量并导致 PhotoLine 溢出内存，从而导致远程代码执行。

具体而言，程序会从 GIF 文件中读取一个短字节值，该值除了会被存在漏洞的 PhotoLine 代码用来计算变量计数器，也将用于包含内存写入指令的内存循环。更多详细信息，请访问此处。

图形交换格式图像文件如今得到广泛使用，是互联网上最常用的图像格式之一。

TALOS-2017-0427

在解析 SVG 文件时，PhotoLine 会使用一个大小参数来执行 memset 函数，该大小参数可能被攻击者利用。具体而言，大小参数根据 SVG 路径的 D 属性计算（该属性是一个字符串，包含一系列可以操纵的路径说明）。此漏洞仅在 feGaussianBlur 过滤器被附加到路径样式时存在。更多详细信息，请访问此处。

可缩放矢量图形图像文件十分常用，是当今互联网上常见的图像格式之一，支持交互性和动画功能。所有主要的网络浏览器都支持显示 SVG 文件。

TALOS-2017-0458

Truevision TGA 通常称为 TARGA，是一种光栅图形文件格式，于八十年代初开发，是第一批个人计算机中最常用的图形格式之一。该格式至今仍在使用。

Computerinsel GmbH Photoline 的 TGA 解析功能中存在内存损坏漏洞。经特殊设计的 TGA 文件引发的漏洞可导致潜在的代码执行。攻击者可发送特定的 TGA 文件来触发此漏洞。更多详细信息，请访问此处。

虽然这些漏洞具体影响的是 Computerinsel PhotoLine 图像编辑软件，但建议其他常用图像编辑程序的用户也安装最新更新以确保自己运行的是最新的程序版本，因为最新版本中包含的安全漏洞数量可能最少。

受影响的版本

已确认 Computerinsel GmbH PhotoLine 版本 20.02 中存在漏洞，但以前的版本中可能也存在漏洞。供应商已发布该软件的更新版本，可从此处下载。

防护

以下 Snort 规则可以检测相关的漏洞攻击活动。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：43725-43726 (TALOS-2017-0387)、44178-44179 (TALOS-2017-0427)、44451-44452 (TALOS-2017-0458)

发布者：VANJA SVAJCER；发布时间：15:05
标签：CVE-2017-12106、CVE-2017-2880、CVE-2017-2920、远程代码执行、漏洞、漏洞聚焦