2017 年 10 月 10 日，星期二

漏洞聚焦：修复了 Simple DirectMedia Layer 中的任意代码执行漏洞

今天，Talos 披露了在 Simple DirectMedia Layer 库中发现的两个漏洞。Simple DirectMedia Layer (SDL) 是一个跨平台开发库，通过提供对音频、键盘、鼠标、游戏杆和图形硬件的低级别访问权限，用于视频播放软件、仿真程序和游戏。借助其 SDL_image 库，SDL 还能够处理各种图像格式（例如 GIMP 的默认分层图像格式 XCF）。

攻击者可以通过 SDL 能够处理的经特殊设计的文件（例如 XCF 文件）利用其中一个漏洞来攻击用户。

鉴于许多应用都会使用 SDL，因此 Talos 与 SDL 社区进行协调，决定披露这些漏洞，并确保更新版本的库可供使用。

漏洞详细信息

本文重点介绍的两个漏洞均由 Yves Younan 发现。

CVE-2017-2887/TALOS-2017-0394 - Simple DirectMedia Layer SDL_image XCF 属性处理代码执行漏洞

我们发现了一个缓冲区溢出漏洞，此漏洞可能会导致在受影响的主机上执行任意代码。出现此漏洞是因为对从文件中读到的数据以及数据的后续使用验证不足。在本例中，从 XCF 图像文件中读取的“id”和“length”属性未经验证即投入使用，可能会导致基于堆栈的缓冲区溢出。

CVE-2017-2888/TALOS-2017-0395 - Simple DirectMedia Layer Create RGB Surface 代码执行漏洞

我们发现了一个整数溢出漏洞，此漏洞可能会导致在受影响的主机上执行任意代码。此漏洞是在通过调用“CreateRGBSurface”函数创建新的 RGB 表面时出现的。如果向此函数传递足够大的宽度和高度值，可能会导致乘法运算溢出，进而导致分配的内存过小。而后，后续的写入也会越界。

有关这些漏洞的完整技术详细信息，请访问我们网站上的漏洞报告门户。

防护

Talos 已发布以下 Snort 规则来解决此漏洞。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信息而有所变更。Firepower 客户应更新 SRU，使用最新的规则集更新。打开源 Snort 用户规则集客户可以在 Snort.org 上下载出售的最新规则包，保持最新状态。

Snort 规则：43855-43856、43858、43860

发布者：ALEXANDER CHIU 发布时间：10:56 AM

标签：防护、SNORT 规则、漏洞研究

分享此文