2017 年 3 月 22 日，星期三

漏洞聚焦：LabVIEW 中的代码执行漏洞

概述

LabVIEW 是 National Instruments 发布的系统设计和开发平台。该软件广泛用于创建数据采集、仪器仪表控制和工业自动化应用。Talos 现披露该软件中存在的一个代码执行漏洞和一个内存损坏漏洞，打开经特殊设计的 VI 文件（LabVIEW 使用的专有文件格式）可触发该漏洞。

TALOS-2017-0269 内存损坏漏洞 (CVE-2017-2775)

在处理输入 VI 文件的“LastSavedTarget”段时，会读取用于循环条件的四个字节，以清除 labView 内部堆结构的块。如果提供了 LvVarientUnflatten 函数，攻击者可以通过无效的循环终止符清除内部堆块，从而可能导致远程代码的执行。

有关完整的详细信息，请点击此处。

已知存在漏洞的版本：LabVIEW 2016 版本 16.0

讨论

对于想要以组织中特定人员和系统为攻击目标的攻击者而言，利用专业文件格式中的漏洞可能是个有用的办法。与所有攻击一样，只有在安装有易受攻击软件的系统上才能利用漏洞。由于 LabVIEW 广泛用于数据采集和控制系统的自动化中，因此成功利用 LabVIEW 漏洞的攻击者就能在控制物理系统的设备上获得一个立足点。

使用此软件和类似软件控制物理系统的组织需要考虑到一种可能性，即攻击者有可能利用控制软件中的漏洞获得物理系统的访问权限。同样，各个组织还应该记住，专有文件格式并不能防范软件漏洞。即使不存在发布的文件格式规范，仍有可能发现由恶意文件触发的漏洞。

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：41370-41371

发布者：MARTIN LEE 发布时间：0:52
标签：CVE-2017-2775、物联网、LABVIEW、NATIONAL INSTRUMENTS、漏洞聚焦