2017 年 8 月 29 日，星期二

漏洞聚焦：LabVIEW 中的代码执行漏洞

漏洞发现者：思科 Talos 团队的 Cory Duplantis

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，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-2017-0273 内存代码执行漏洞 (CVE-2017-2779)

VI 文件格式描述了在 LabVIEW 中实施的各种系统。虽然该文件格式没有已发布的规范，但通过检查文件可以发现文件中包含一个名为“RSRC”的部分（很可能包含资源信息）。调整 VI 文件中此部分的值可能会导致受控的循环条件，进而导致任意 NULL 写入。此漏洞可以被攻击者用来创建经特殊设计的 VI 文件。打开该文件时，便会导致执行攻击者提供的代码。

有关该漏洞的完整详细信息，请点击此处。

National Instruments 并不认为此问题构成了其产品的漏洞，由于任何.exe 类文件格式都可以遭到修改，将合法内容替换为恶意内容，因此他们拒绝发布补丁。Talos 对此保留不同意见。该漏洞与 .NET PE 加载程序漏洞 CVE-2007-0041（已通过 MS07-040 修复）之间存在相似之处。此外，许多用户可能并未意识到 VI 文件类似于.exe 文件，应给予相同的安全要求。

已知存在漏洞的版本：
LabVIEW 2016 版本 16.0

讨论

此前，我们已披露了同一软件中的漏洞。正如此前披露的漏洞，各个组织应该意识到，虽然专有文件格式没有已发布的规范，但仍然应该对其进行检查，以便发现漏洞。针对与物理世界（如数据收集与控制系统）交互的系统发起的攻击一旦得手，可能会给安全带来严重影响。部署此类系统、甚至将其作为试点项目的组织，应意识到这些漏洞（如上述漏洞）所带来的风险，并充分保护系统。

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 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：41368 - 41369

发布者：MARTIN LEE 发布时间：11:09 AM
标签：CVE-2017-2779、LABVIEW、NATIONAL INSTRUMENTS、TALOS-2017-0273、VI 文件、漏洞、漏洞聚焦