2017 年 9 月 13 日，星期三

漏洞聚焦：LibOFX 标签解析代码执行漏洞

漏洞发现者：Talos 团队的 Cory Duplantis

概述

LibOFX 是一种依照 OFX （开放金融交换）标准实现的开源库，金融机构使用这种开放格式与客户分享金融数据。作为复杂标准的一种实现方式，该库已被 GnuCash 等各种金融软件所使用。Talos 在该库中发现了一个可被利用的缓冲区溢出漏洞：攻击者利用经特殊设计的 OFX 文件可以导致越界写入，从而在受影响的设备上执行任意代码。此漏洞目前尚未得到修补。在供应商漏洞报告和披露政策规定的期限内，Talos 也未收到开发者的任何回复。

TALOS-2017-0317 (CVE-2017-2816) - LibOFX 标签解析代码执行漏洞

具有讽刺意味的是，此漏洞存在于 sanitize 函数解析标签的过程中。在该函数中，标签名称存储在本地的堆栈中（标签名过长会导致栈溢出）。

有关详细信息，请参阅漏洞报告：TALOS-2017-0317

测试版本：LibOFX 0.9.11

讨论

作为开源库，LibOFX 可能会用于各种金融应用中。此漏洞为攻击者提供了许多诱人的机会。触发此漏洞不需要用户交互，而存在此漏洞的系统很可能包含有价值的金融信息，一旦被盗，有可能会被用于身份盗用或欺诈，甚至会被直接转卖给其他犯罪者。

组织可能并不知道该库已被第三方软件或内部开发的软件用来解析 OFX 文件。组织应跟踪内部软件中使用的开源库，或尽快应用第三方供应商提供的补丁，这对于妥善管理此类对攻击者极具诱惑力的漏洞至关重要。

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：42277-42278

发布者：VANJA SVAJCER 发布时间：10:24 AM
标签：OFX、开放金融交换、远程代码执行、漏洞、漏洞聚焦