2017 年 11 月 15 日，星期三

漏洞聚焦：libxls 中的多个远程代码执行漏洞

思科 Talos 团队的 Marcin Noga 发现的漏洞

Talos 团队发布了在 libxls 库中发现的七个新漏洞：TALOS-2017-0403、TALOS-2017-0404、TALOS-2017-0426、TALOS-2017-0460、TALOS-2017-0461、TALOS-2017-0462 和 TALOS-2017-0463。这些漏洞会导致攻击者通过利用经特殊设计的 XLS 文件来远程执行代码。

概述

libxls 是一个在 Windows、Mac 和 Linux 系统上受支持的 C 语言库，它可以读取 Microsoft Excel 文件格式 (XLS) 的文件，从当前版本的 xls 文件到 Excel 97 (BIFF8) 格式。
该库由“readxl”包使用，后者可通过 CRAN 代码库安装在 R 编程语言中。该库也是“xls2csv”工具的一部分。该库还可用于成功解析 Microsoft XLS 文件。

请注意，目前仅可通过 svn 获取更新。

详情

TALOS-2017-0403

在 libxls 1.4 的 xls_mergedCells 函数中存在可利用的越界写入漏洞。通过利用经特殊设计的 XLS 文件可以引起内存损坏，导致远程代码执行。攻击者可以发送恶意的 XLS 文件来触发此漏洞，将其作为使用邮件的网络钓鱼活动的一部分发送，来入侵受害者的计算机。

点击此处获取完整的技术建议。

TALOS-2017-0404

libxls 1.4 的 read_MSAT 函数中存在可利用的越界写入漏洞。
通过利用经特殊设计的 XLS 文件可以引起内存损坏，导致远程代码执行。
攻击者可以发送恶意的 XLS 文件来触发此漏洞，将其作为使用邮件的网络钓鱼活动的一部分发送，来入侵受害者的计算机。

点击此处获取完整的技术建议。

TALOS-2017-0426

libxls 1.3.4 的 xls_getfcell 函数中存在可利用的基于堆栈的缓冲区溢出漏洞。通过利用经特殊设计的 XLS 文件可以引起内存损坏，导致远程代码执行。攻击者可以发送恶意的 XLS 文件来触发此漏洞，将其作为使用邮件的网络钓鱼活动的一部分发送，来入侵受害者的计算机。

注意：此漏洞不会影响可在 R 编程语言中安装的 readxl 包。

点击此处获取完整的技术建议。

TALOS-2017-0460

在处理 MULBLANK 记录时，libxls 1.4 的 xls_preparseWorkSheet 函数中存在可利用的整数溢出漏洞。通过利用经特殊设计的 XLS 文件可以引起内存损坏，导致远程代码执行。攻击者可以发送恶意的 XLS 文件来触发此漏洞，将其作为使用邮件的网络钓鱼活动的一部分发送，来入侵受害者的计算机。

点击此处获取完整的技术建议。

TALOS-2017-0461

在处理 MULRK 记录时, libxls 1.4 的 xls_preparseWorkSheet 函数中存在可利用的整数溢出漏洞。通过利用经特殊设计的 XLS 文件可以引起内存损坏，导致远程代码执行。攻击者可以发送恶意的 XLS 文件来触发此漏洞，将其作为使用邮件的网络钓鱼活动的一部分发送，来入侵受害者的计算机。

点击此处获取完整的技术建议。

TALOS-2017-0462

libxls 1.4 的 xls_appendSST 函数中存在可利用的整数溢出漏洞。通过利用经特殊设计的 XLS 文件可以引起内存损坏，导致远程代码执行。攻击者可以发送恶意的 XLS 文件来触发此漏洞，将其作为使用邮件的网络钓鱼活动的一部分发送，来入侵受害者的计算机。

点击此处可获得完整的技术建议。

TALOS-2017-0463

libxls 1.4 的 xls_addCell 函数中存在可利用的越界漏洞。通过利用经特殊设计的 XLS 文件可以引起内存损坏，导致远程代码执行。攻击者可以发送恶意的 XLS 文件来触发此漏洞，将其作为使用邮件的网络钓鱼活动的一部分发送，来入侵受害者的计算机。

注意：此漏洞不会影响可在 R 编程语言中安装的 readxl 包。

点击此处可获得完整的技术建议。

产品网站：
http://libxls.sourceforge.net/

防护

已发布以下 Snort ID 来检测这些漏洞：44101-44102、44092-44093、44163-44164、44520-45523、44593-44594、44589-44590

发布者：NICK BIASINI 发布时间：10:36
标签：零日、TALOS、漏洞研究、漏洞聚焦