2017 年 2 月 24 日，星期五

漏洞聚焦：多个 Ichitaro Office 漏洞

漏洞发现者：思科 Talos 团队的 Cory Duplantis 和另一位成员

Talos 在 Ichitaro Office 套件中发现了三个漏洞。Ichitaro 由 JustSystems 发布，是公认的日本比较常用的一款文字处理软件。报告的三个漏洞全部会导致代码执行。这几个问题最初于 9 月报告给供应商，他们直到 2 月 23 日才解决这些问题。

TALOS-2016-0196 (CVE-2017-2789) - Ichitaro Office JTD 图表处理代码执行漏洞
TALOS-2016-0197 (CVE-2017-2790) - Ichitaro Office Excel 文件代码执行漏洞
TALOS-2016-0199 (CVE-2017-2791) - Ichitaro Word Processor PersistDirectory 代码执行漏洞

有关这些问题可能如何遭到普遍利用的深入技术分析，请点击此处参阅相关文章。

详细信息

TALOS-2016-0196

Ichitaro 的专有文件格式是称为 .jtd 的复合文档，类似于 Microsoft Word 的 .doc。处理 .jtd 中的图表流时，该应用会在解析图表时分配空间。将文件数据复制到此缓冲区中时，该应用会计算两个值，以确定要从文档中复制多少数据。如果这两个值都大于缓冲区的大小，该应用将选择二者中较小者，并相信它从文件复制数据。如果复制的数据量大于缓冲区大小，这会导致基于堆的缓冲区溢出。此溢出会损坏指针算法中用于写入数据的堆中的偏移量，并可能导致在该应用环境中执行代码。更多详细信息，请访问此处

TALOS-2016-0197

Ichitaro 可处理 Microsoft Excel 的 .xls 文件格式。处理 .xls 文件工作簿流中的记录类型 0x3c 时，该应用相信是大小大于零的，从长度中减去一，并使用此结果作为 memcpy 的大小。攻击者可以利用这一点创建一个文件，打开该文件时会导致基于堆的缓冲区溢出，并可能导致在该应用环境中执行代码。更多详细信息，请访问此处

TALOS-2016-0199

Ichitaro Office 在尝试打开经特殊设计的 PowerPoint 文件时存在漏洞。由于该应用无法正确处理某个函数错误情况，该应用会在指针计算中使用此结果读取文件数据。这会导致该应用将文件中的数据读取到无效地址，从而损坏内存。在适当条件下，这可能导致在该应用环境中执行代码。更多详细信息，请访问此处

测试版本

JustSystems Ichitaro 2016

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：41110-41111、40125-40156 和 40490

发布者：WARREN MERCER；发布时间：10:06
标签：零日、远程代码执行、VULNDEV、漏洞聚焦