2016 年 7 月 20 日，星期三

漏洞聚焦：Oracle Outside In Technology 漏洞汇总

漏洞发现者：Aleksandar Nikolic。作者：Jaeson Schultz 和 Aleksandar Nikolic。

对许多软件程序来说，它们所执行的最基本任务都会涉及文件的读取、写入和一般处理。在如今高度网络化的环境中，文件及文件处理程序几乎无处不在，例如 FTP 传输、HTTP 表单上传、邮件附件等等，不一而足。

鉴于计算机用户需要经常与种类如此繁多的文件进行交互，Oracle Corporation 设计了专门的工具来协助编程人员编写支持此类日常任务的软件：Outside In Technology (OIT)。OIT 网站上对该软件的描述是：“Outside In Technology 是一套软件开发工具包 (SDK)，它为开发人员提供了一个提取、规范化、清理、转换和查看 600 多种非结构化文件格式的内容的综合解决方案。”

在 4 月份，Talos 发布的一篇博客中介绍了 Oracle 修补的一个与 OIT 相关的任意代码执行漏洞。由于有大量第三方产品会使用 Oracle 的 OIT 来解析和转换文件，所以该漏洞以及本博客中披露的其他 18 个 OIT 漏洞会导致严重的后果。2016 年 1 月的一篇有关 OIT 的 CERT 公告中公开了许多受影响的第三方产品列表，特别值得注意的是其中包括一些安全和消息传送相关产品。根据 CERT 的公告，依赖 Oracle Outside In SDK 的产品列表包括：

- Avira AntiVir for Exchange - 面向 Microsoft Exchange 的防病毒保护
- IBM WebSphere Portal - 用于提供企业 Web 门户
- Google Search Appliance - 用于通过单一搜索框搜索企业内的所有内容
- Guidance Encase - 调查分析软件
- Microsoft Exchange - 企业邮件和工作效率软件
- Novell Groupwise - 面向大型企业的协作工具
- Raytheon SureView - 专为企业可视性和用户活动监控设计的软件
- Veritas (Symantec) Enterprise Vault - 一款通过归档进行信息管理的程序

Talos 尚未确认是否上面列出的每一款第三方产品都会受到影响。但是，我们已确认其中一些产品运行了与 OIT 相关的存在漏洞的代码。例如，如果在 Microsoft Exchange 2013（或更低版本）中启用 WebReady Document Viewing，攻击者可以通过向受害者发送恶意邮件附件，诱使受害者使用 Web 预览功能打开邮件，从而利用这些漏洞。

此外，如果启用 Data Loss Prevention，攻击者可以通过从受影响的 Exchange 服务器发送带有恶意附件的邮件，来触发漏洞。如果安装了 Avira AntiVir for Exchange（v12.0.2775.0 或更低版本），那么仅仅是发送或接收恶意邮件便会触发漏洞，因为该程序会扫描所有入站和出站邮件。此外，攻击者还能以连锁反应的方式更有效地利用多个 OIT 漏洞。因此，Talos 建议用户直接关注这些供应商的最新通知，了解有关这些漏洞影响范围的更多信息。

目录

1. PDF /Size 整数溢出
Talos-2016-0097 (CVE-2016-3575)

尾部对象用于指示“交叉引用表和某些特殊对象在文件正文中的位置”。其中包括多种字段，如 /ID、/Root、/Size 和 /Info。/Size 用于保留 PDF 中的对象数量。

Key	Value type	Value
/Size*	Integer	Total number of entries in the file's cross-reference table (usually equal to the number of objects in the file plus one).
/Root*	Indirect reference to dictionary	The *document catalog*.
/Info	Indirect reference to dictionary	The document's *document information dictionary*.
/ID	Array of two Strings	Uniquely identifies the file within a work flow. The first string is decided when the file is first created, the second modified by workflow systems when they modify the file.

尾部字典中的条目（*表示必填条目）

较大的 /Size 将导致 Oracle OIT PDF 解析器出现问题。尽管 Oracle 的解析器会检查整数溢出，但是在后续步骤中会将结果乘以 4（左移赋值），因而导致之前溢出检查提供的所有保护失效。

```
.text:B74ECE59    mov       edi,   eax     [1]
.text:B74ECE5B    shl       edi,   4       [2]
.text:B74ECE5E    mov       [esp+6BCh+s],   edi
.text:B74ECE61    call      _SYSNativeAlloc              [3]
.text:B74ECE66    mov       edx,   [esp+6BCh+arg_10]
.text:B74ECE6D    mov       [edx+1D6Ch],   eax       [4]
.text:B74ECE73    test      eax,   eax
.text:B74ECE75    jz        loc_B7
```

在 [1] 中，“eax”中的值直接来自 /Size 元素的 32 位舍入值。在 [2] 中，其结果被乘以 4，因此会使之前执行的整数溢出检查失效。在 [3] 中，指令调用了“malloc”封装程序，并将返回的指针保存在 [4] 中。如果 /Size 值经过特殊选择，可能会导致第一个基本块的 [2] 中出现整数溢出，使较小的值被传递到 [3] 中的 SYSNativeAlloc。当出于舍入的原因，堆分配器将指针返回至比预期更大的堆数据块时，便会发生此问题。

例如，如果 /Size 值指定为 0x10000001，则会在分配前通过检查，但当此值移动 4 位时，将变为 0x10，从而使分配变小。但是根据底层分配器，分配的数据块的实际大小会更高。对于 Linux，返回的数据块长度为 24 字节，且后续的“memset”将仅初始化前 16 个字节。如果仅初始化缓冲区的前 16 个字节，代码将访问未初始化为零的内存。未初始化的内存中存在的剩余数据可造成内存损坏，从而可能导致代码执行。

2. TIFF ExtraSamples 代码执行 Talos-2016-0103 (CVE-2016-3581)

TIFF 文件也能够触发可导致远程代码执行的漏洞。当解析图像文件目录 (IFD) 中存在的带“ExtraSamples”标签的 TIFF 文件时，如果堆中的内存分配不足，Oracle OIT SDK 中便会产生此漏洞。在这种情况下，ImageWidth、SamplesPerPixel、BitsPerSample 和 ExtraSamples 值被视为是 TIFF 文件的标准值，但是包含 ExtraSamples 是触发此漏洞的关键。由于其他位并不在分配的考虑范围内，所以包含 ExtraSamples 标签会导致可能的基于堆的溢出。

3. TIFF 光度解析代码执行 Talos-2016-0104 (CVE-2016-3582)

1992 年，TIFF 文件格式规范更新，并添加了扩展项来支持新的图像类型。最初，TIFF 文件仅支持四种图像类型；黑白、灰阶、RGB 和调色板彩色。更新后的 TIFF 规范包括一种新的 CMYK（分色）图像类型。要指定 TIFF 图像类型，需使用“PhotometricInterpretation”字段。将“PhotometricInterpretation”级别设置为 5（CMYK/分色格式）的 TIFF 文件将导致 Oracle SDK 在与其他设置进行比较时遵从替代代码路径。此替代代码路径允许将 ImageWidth 值用于未检查的分配，最终造成堆溢出。

4. GIF ImageWidth 代码执行
Talos-2016-0105 (CVE-2016-3583)

除了 PDF 和 TIFF，GIF 文件也可能会导致危险。ImageWidth 值应说明特定 GIF 的绝对宽度，并且小于同一文件中出现的逻辑屏幕宽度值。当解析图像描述符块中 ImageWidth 设置为 0xFFFF 的 GIF 图像时，将会触发 Oracle 的 Outside In SDK 中的这个漏洞。将 ImageWidth 设置为 0xFFFF 会触发整数溢出，导致在 libvs_gif.so 中同一函数的两个分支中产生越界内存写入。

5. Gem_Text 代码执行
Talos-2016-0162 (CVE-2016-3595)

GEM 元文件是在矢量绘图程序 Gem Draw 中渲染图片的说明文件。在 Oracle Outside In Technology libim_gem2 库的文件解析代码中存在整数溢出漏洞。当解析 GEM 元文件数据时，会执行未经检查的内存分配。因此，经特别制作的 Gem 文件可触发整数溢出，导致多个基于堆的缓冲区溢出，而且可能导致远程代码执行。

6. PSI 文件整数溢出代码执行
Talos-2016-0161 (CVE-2016-3594)

在 Oracles 的 Outside In Technology libim_psi2 库中存在解析漏洞。具体而言，存在整数溢出，可导致错误的内存分配，然后导致大型内存复制操作。当解析 PSI 图像文件时，会读取 2 字节大小的字段并对其进行符号扩展。然后此值会用于内存分配以及后续的“memmove”调用。分配内存区之前读取的大小值会增加 8 倍，但原始大小会用“memmove”调用。

7. Word DggInfo 代码执行
Talos-2016-0160 (CVE-2015-6014) *2016 年 1 月已修复

当解析包含经特殊设计的 DggInfo 元素内容的错误格式 OLE 文件时，便会触发 Escher 图片解析库 libvs_eshr 中的漏洞。当 DggContainer 第一个子项的 ID 从 0xF006 (Dgg) 更改为 0xF007 (BSE) 时，会导致解析器混乱，最终，文件中的 4 字节值会被用作“cmp”指令中的指针。如果比较失败，间接“call”指令中会使用同一指针，从而导致任意代码执行。

8. Mac Works Database VwStreamSection 代码执行 Talos-2016-0159 (CVE-2016-3593)

当解析 Mac Works Database 文档时，OIT 会使用计数器循环写入内存，其中该计数器包含从文件中某个字节读取的上限值。由于执行算法运算后不会执行任何大小检查，所以可能导致越界内存写入。

9. Mac Word ContentAccess libvs_word+63AC 代码执行 Talos-2016-0158 (CVE-2016-3592)

当解析 Mac Word 文档时，OIT 会将文件中的单字节值用作内存访问算法运算中所使用计数器的起始值。由于执行算法运算后不会执行任何大小检查，所以可能导致越界 4 字节内存写入。

10. BMP 堆缓冲区溢出和代码执行 Talos-2016-0163 (CVE-2016-3596)

当解析经特殊设计的 ICO 文件时，未经检查的位图宽度指定值会被用于计算内存写入操作的大小。压缩方法必须设置为 0x01 或 BI_RLE8。当读取文件时，堆中的内存片段实际上会被零覆盖。此覆盖大小未经检查，直接来自位图宽度。这可能会导致堆数据结构被空字节覆盖。在所提供的测试案例中，越界空字节写入会覆盖函数指针，从而导致系统崩溃。攻击者可以通过蓄意调整覆盖大小，操纵堆中的函数指针，实现任意代码执行。

11. Mac Works VwStreamReadRecord 内存损坏 Talos-2016-0157 (CVE-2016-3591)

当解析 Mac Works Database 文档时，OIT 会以目标地址计算中的计数器循环写入内存。由于执行算法运算后不会执行任何大小检查，所以可能导致不完全受控的 2 字节覆盖。

此漏洞出现在 libvs_mwkd.so 库（映像基址为 0xB7F89000）的“VwStreamReadRecord”函数中，特别是以如下基本块开始的函数：

```
.text:B7F8ACF6          movzx   eax, [esp+3Ch+var_12]
.text:B7F8ACFB          mov     edx, [edi+31Ch]
.text:B7F8AD01          mov     ecx, ebp
.text:B7F8AD03          mov     [edx+eax], cl
.text:B7F8AD06          movzx   eax, word ptr [esp+3Ch+var_10] [1]
```

```
.text:B7F8AD0B          movzx   esi,  [esp+3Ch+var_12] [2]
.text:B7F8AD10          mov     [edi+eax*2+298h],  si [3]
.text:B7F8AD18          add     word ptr [esp+3Ch+var_10],  1
.text:B7F8AD1E          add     esi,  1
.text:B7F8AD21          mov     [esp+3Ch+var_12],  si
.text:B7F8AD26          cmp     bp,  0F9h
.text:B7F8AD2B          ja      loc_B7F8AE1A
.text:B7F8AD31          test    bp,  bp
.text:B7F8AD34          jz      loc_B7F8ADEB
.text:B7F8AD3A          mov     [esp+3Ch+var_1A],  0
.text:B7F8AD41          jmp     short loc_B7F8AD71
```

在 [1] 和 [2] 中，“eax”和“esi”的预计算值是从堆栈中读取的，并使用零进行扩展。在 [3] 中，“eax”用于目标地址计算，并且在此写入“si”的值。“eax”和“esi”的初始值也相关，其中“eax”充当计数器。由于没有界限检查，所以可能导致 2 字节越界覆盖。

攻击者可以利用经特殊设计的文件，将所要释放的指针转移到自己控制的区域，然后使用该区域破坏“free()”并实现代码执行。

12. PDF /Kids 信息泄漏 Talos-2016-0096 (CVE-2016-3574)

PDF 文档页面是通过页面树访问的，页面树定义了文档中的所有页面。页面树的每个节点通常包含 /Type、/Parent、/Kids 和 /Count 条目。/Kids 引用用于指定可从当前节点直接访问的所有子元素。

但是，在 Oracle OIT PDF 解析器处理 /Kids 引用的方式中存在一个漏洞。当解析对象中包含错误格式的 /Kids 引用的 PDF 文件时，紧接在 /Kids 后的值会被解析为字符串，其中应存在一个引用阵列。这会导致解析器要求从文件中读取的字符串所在位置的指针，导致任意读取访问冲突。在格式正确的 PDF 文件中，/Kids 元素后跟随的阵列必须至少包含一条引用。此漏洞出现在 libvs_pdf.so（基地址为 0x0xB74BF000）中：

```
.text:B74E71DB  mov     eax,  [eax]  [1]
.text:B74E71DD  mov     edi,  [esp+5Ch+var_24]
.text:B74E71E1  mov     eax,  [eax+edi*4]  [2]
.text:B74E71E4  mov     [esp+5Ch+var_4C],  eax
```

```
.text:B74E71E8    mov       ecx,   [esp+5Ch+var_34]
.text:B74E71EC    mov       edx,   [esp+5Ch+var_48]
```

在 [1] 中，“eax”指向从文件复制到堆中的字符串。此字符串中的前四个字节用于 [2] 中的内存访问计算，导致任意读取访问冲突。如果 [2] 中计算的值最终指向有效内存，将会在受到控制的地址读取成功。但是，如果 /Kids 元素后的值为纯整数，则会到达不同的代码路径并将整数值解析为指针，从而导致在以下位置发生完全受到控制的任意读取。

```
.text:B74E718A    mov       eax,   [esp+5Ch+var_18]
.text:B74E718E    mov       eax,   [eax]
.text:B74E7190    xor       edx,   edx
.text:B74E7192    mov       edi,   [eax+4]    [1]
.text:B74E7195    test      edi,   edi
.text:B74E7197    jz        loc_B74E72A2
```

13. PDF 空指针取消引用拒绝服务 Talos-2016-0098 (CVE-2016-3576)

当解析经特殊设计的 PDF 文档时，OIT 会发生空指针取消引用，从而导致进程终止。解析器成功解码 /FlateDecode 编码流数据后，将会继续执行其中包含的运算符。当执行流中包含的一部分文本中的“Tj”运算符时，将会引用可能包含字符集映射的内存结构。不会执行空指针检查，且由于结构被初始化为零，这可能导致系统崩溃。

14. PDF 递归堆栈溢出拒绝服务 Talos-2016-0099 (CVE-2016-3577)

PDF 文档层次结构的根为目录字典，可通过 PDF 文件尾部对象中的 /Root 条目进行定位。目录字典必须具有 /Catalog 类型。当解析的错误格式 PDF 文件包含对具有错误格式 xref 表格或缺少 xref 表格的 /Root 元素的引用时，每次都会使用相同的参数对函数执行递归调用。这最终会由于处理堆栈耗尽而导致系统崩溃。

15. PDF /FlateDecode /Colors 拒绝服务 Talos-2016-0100 (CVE-2016-3578)

当解析的 PDF 文件包含 /Predictor 设置为 1 以外的其他值的 /FlateDecode 编码流时，错误格式的 /Colors 值会导致在取消解码器初始化时在 libsc_ut.so 库中产生空指针取消引用。

16. PDF /Type /Xref 拒绝服务 Talos-2016-0101 (CVE-2016-3579)

当解析的 PDF 文件具有包含流的对象时，缺少对象类型规范会导致任意指针访问。/Type 元素后出现的 ASCII 整数值会转换为 32 位整数，并且随后用作比较运算中的指针。在指针无效的情况下，会发生进程崩溃。

17. PDF Xref 偏移拒绝服务 Talos-2016-0102 (CVE-2016-3580)

OIT SDK 的 PDF 解析器中存在一个漏洞，可导致在某些情况下发生未经检查的内存分配操作之后，出现越界堆内存访问。

在 PDF 文件中，xref 表包含多行，每行包含三个值（第一行除外，此行用于指定引用的第一个对象以及对象数量）。第一个值表示相对于发现对象的文件的 10 位偏移量。在经特殊设计的 PDF 文件中，OIT PDF 解析器将指定值用作可能失败的“realloc()”调用中的参数。系统会检查返回值中的错误，但之后会忽略该值。然后会将初始数字值用作进程清除期间发生越界读取的循环中的上限值。

18. Mac Word ContentAccess libvs_word 拒绝服务 Talos-2016-0156 (CVE-2016-3590)

当解析 Mac Word 文档时，OIT 会将文件中的单字节值用作内存访问算法运算中所使用计数器的最大值。算法运算后不会执行任何大小检查，从而导致越界内存访问。计算的内存地址会用作“or byte”指令中的目标操作数。

结论

如果软件将不受信任的数据作为输入，而不对其进行正确和必要的验证，则会接二连三不断发生问题。此外，并非所有软件开发人员都熟悉现有的大量文件格式，因此他们不得不依赖 Oracle 的 OIT 等 SDK。但是遗憾的是，如果在第三方采用的 SDK 中发现漏洞，则需要更多的时间来进行修补：首先，由维护此 SDK 的组织发布补丁，经过一段时间之后，采用此 SDK 的第三方才会向其客户提供包括这些修复的更新。这就为恶意攻击者提供了利用第三方产品中漏洞的大好时机。

发布者：Jaeson Schultz；发布时间：14:40

标签：Oracle、漏洞、漏洞聚焦