2016 年 6 月 8 日，星期三

漏洞聚焦：Google Chrome 网络浏览器中的 PDFium 漏洞

此漏洞的发现者为思科 Talos 的 Aleksandar Nikolic。

PDFium 是 Google Chrome 网络浏览器内置的默认 PDF 阅读器。Talos 发现 PDFium PDF 阅读器中存在可被利用的堆缓冲区溢出漏洞。当用户查看包含嵌入式 jpeg2000 图像的 PDF 文档时，攻击者即有机会在用户的系统中执行任意代码。对威胁实施者而言，最有效的攻击手段是将一个恶意 PDF 文件放在某个网站上，然后利用网络钓鱼邮件或恶意广告将受害者重定向至此网站。

TALOS-CAN-0174 堆缓冲区溢出漏洞 (CVE-2016-1681)

在 Chrome 的 PDF 渲染引擎 PDFium 所使用的 jpeg2000 图像解析器库中，存在一个堆缓冲区溢出漏洞。此漏洞位于底层 jpeg2000 解析库 OpenJPEG 中，但是就 Chrome 而言，
由于构建过程比较特殊，所以此漏洞可能被攻击者利用。

在独立版本中，OpenJPEG 库中现有的断言调用可防止出现堆溢出，但是在 Chrome 发行版本中的一些版本中，却不提供断言调用。漏洞的来源位于“j2k.c”文件中的函数“opj_j2k_read_siz”的以下代码中：

```
        for     (i = 0; i < l_nb_tiles; ++i) {
                l_current_tile_param->tccps = (opj_tccp_t*) opj_calloc(l_image->numcomps, sizeof(opj_tccp_t));
                if (l_current_tile_param->tccps == 00) {
                        opj_event_msg(p_manager, EVT_ERROR, "Not enough memory to take in charge SIZ marker\n");
                        return OPJ_FALSE;
                }

                ++l_current_tile_param;
        }
```

如果在对“opj_calloc”（“calloc”包装程序）的上述调用中，“numcomps”值为零，“calloc”将返回一个稍后可以传递给“free”的唯一指针（这取决于实施，不过在现代 Linux 操作系统中会发生这种情况）。“calloc”返回的唯一指针通常为小内存分配（对于 64 位代码而言，分配 0x20 字节）。在使用此缓冲区时，这可能导致随后代码出现堆缓冲区溢出。当取消引用之前分配的缓冲区时，“opj_j2k_read_SQcd_SQcc”函数中会发生溢出。越界内存写入首先出现在以下代码中：

```
                l_tccp->qntsty = l_tmp & 0x1f;
                l_tccp->numgbits = l_tmp >> 5;
```

在上述代码中，“l_tccp”指针将指向之前错误分配的区域。在后续的越界写入过程中，在以下代码中会取消引用该结构。

发生此溢出的首要条件是组件数量为 0。实际上，这种情况会在函数开头的断言中得到检查：

```
        assert(p_comp_no <  p_j2k->m_private_image->numcomps);
```

如果满足错误分配的必要条件，上述断言将失败（在默认版本的 OpenJPEG 库中确实发生过这种情况）。但是，由于 Chrome 和 PDFium 的发行版本已删除这些断言，所以有可能导致达到缓冲区溢出点。Talos 已创建了一个包含嵌入式 jpeg2000 的 PDF 文件。此 jpeg2000 图像的 SIZ 标记已被截断（SIZ 标记开始部分为 0xFF51）。因为 SIZ 标记中指定的组件的数量为 0，且此标记后面没有单个组件信息，这会缩短正在解析“opj_j2k_read_siz”中的 jpeg 文件的代码，导致对“calloc”进行所需的错误调用。有效的 jpeg2000 文件和触发此漏洞的 jpeg2000 文件之间的唯一区别是 SIZ 标记指定 0 个组件。

供应商已通过将有问题的“断言”更改为返回错误的“if”语句来解决此漏洞。

测试版本：

在我们的测试中，Talos 测试了 Google Chrome 的以下版本。

Google Chrome 50.0.2661.94 和 PDFium 的 git 版本

结论：

用户在浏览网页时经常会浏览 PDF 文件。攻击者很容易利用此漏洞进行攻击。本着负责任的态度，Talos 和 Google 共同披露了此漏洞（请查看谷歌错误跟踪器）。强烈建议用户务必运行 Google Chrome 浏览器的最新版本。Google Chrome 浏览器可以自动更新，但您仍需要重新启动浏览器，才能启用最新版本。

此漏洞是通过 SID 39161 和 39162 检测到的。

有关最新的 SID 列表，请访问 FireSIGHT 管理中心防御中心。如需获取更多有关零日攻击或漏洞的报告和信息，请访问：

http://talosintel.com/vulnerability-reports/

时间表：

2016 年 5 月 19 日：报告漏洞
2016 年 5 月 19 日：确认漏洞
2016 年 5 月 20 日：修复漏洞，并在 Chromium 中公布修补程序
2016 年 5 月 25 日：在 Chrome Stable 51.0.2704.63 中配置漏洞修补程序
2016 年 6 月 8 日：Talos 发布详细信息
发布者：Earl Carter；发布时间：下午 4:27
标签：CVE-2016-1681、补丁、漏洞聚焦