2016 年 10 月 26 日，星期三

漏洞聚焦：Iceni Argus 缓冲区溢出

Talos 在 Iceni Argus PDF 内容提取软件 中发现了两个基于堆栈的缓冲区溢出漏洞（TALOS-2016-0200 和 TALOS-2016-0202）。此软件用于将 PDF 文档转换为各种基于 xml 的标记格式（例如 XHTML）。一些软件（例如 MarkLogic）在搜索和渲染基于 Web 文档时，会使用 Iceni Argus 执行 PDF 文档转换。这两个漏洞都存在于 PDF 到 html 转换器功能中。通过发送或提供经过精心设计，会导致缓冲区溢出的 PDF 文件，攻击者可以触发其中任何一个漏洞，进而导致任意代码执行。

CVE-2016-8333 (TALOS-2016-0200) Iceni Argus ipfSetColourStroke 代码执行

CVE-2016-8335 (TALOS-2016-0202) Iceni Argus ipNameAdd 代码执行

详细信息

Iceni Argus 执行“ipfSetColourStroke”函数的过程存在 CVE-2016-8333 漏洞。此函数调用的“getRealArgArray”会尝试复制“opStack”容器的元素，但不会验证源阵列的长度是否大于目标阵列。目标阵列的最大长度固定为 9 个 4 字节阵列值。PDF 标头中的数据会定义“opStack”的元素，而异常的 PDF 会造成源中包含 9 个以上元素的情况，这会造成缓冲区溢出，进而导致任意代码执行。

CVE-2016-8335 存在于 Iceni Argus 的 ipNameAdd 功能中。检查此函数，很容易就能发现有问题的代码行。该函数中包含以下代码行

```
strcpy(dest, src);
```

此命令的前面没有对所调用的参数执行任何检查。大家都知道，这是缓冲区溢出的典型示例。令人惊讶的是，长度检查在 strcpy 调用之后才出现，这让它变得完全没有效果。但是要利用溢出，恶意 PDF 必须定义一个不属于“规则”命名对象（以“/”开头的对象）的“令牌”，因为“规则”命名对象在执行期间永远无法到达 strcpy 代码行。

测试版本

CVE-2016-8333

Iceni Argus 版本 6.6.04（2012 年 9 月 7 日）NK

CVE-2016-8335

Iceni Argus 版本 6.6.04（2012 年 9 月 7 日）NK - Linux x64
Iceni Argus 版本 6.6.04（2014 年 11 月 14 日）NK - Windows x64

防护

为了保护我们的客户，Talos 已经发布了相关规则来检测利用该漏洞的攻击尝试。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：40336-40337、40484-40487

完整漏洞报告

http://www.talosintelligence.com/reports/2016-TALOS-0200/
http://www.talosintelligence.com/reports/2016-TALOS-0202/

发布者：WARREN MERCER；发布时间：12:40
标签：零日、ARGUS、ICENI、VULNDEV