2017 年 2 月 27 日，星期一

漏洞聚焦：Iceni Argus PDF 内容提取产品中影响 MarkLogic 的多个远程代码执行漏洞

漏洞发现者：Talos VulnDev 团队的“冰壁”Marcin Noga 和另一位成员。

概述

Talos 发现了 Iceni Argus PDF 内容提取产品中的多个漏洞。攻击者可以利用这些漏洞完全控制受害者的计算机。虽然主要产品已被 Iceni 弃用，但是库仍然受到支持。Iceni 已发布修复这些漏洞的修复版本。不过，库的使用非常广泛；例如，MarkLogic 产品在基于 Web 的文档搜索和呈现过程中，就使用 Iceni Argus 进行 PDF 文档转换。

详细信息

MarkLogic 的转换工具使用 Iceni 的 Argus PDF 库，我们在其中发现了下述漏洞：

TALOS-2016-0210/CVE-2016-8385 - 当用户尝试将恶意 PDF 转换为使用格式不正确的颜色的 XML 时，就会出现此漏洞。返回的指针保持未初始化的状态，稍后会导致基于栈的缓冲区溢出。这可能导致以与本地用户相同的权限执行代码。

TALOS-2016-0211/CVE-2016-8386 是基于堆的缓冲区溢出，如果 PDF 内部嵌入经特殊设计的 truetype 字体文件并且用户尝试将此 PDF 转换为 XML，就会出现此漏洞。该恶意字体可能导致缓冲区初始化大小不足的情况。此情况稍后可能会导致一个溢出条件，攻击者可利用它以与本地用户相同的权限执行代码。

TALOS-2016-0212/CVE-2016-8387 是 LZW 解码器中基于堆的缓冲区溢出。由于缺少界限检查，如果用户尝试转换一个格式错误的 PDF，且该 PDF 中包含的对象使用多个编码类型（以 LZW 类型结束）进行编码，就会触发该漏洞。这可能导致以与本地用户相同的权限执行代码。

TALOS-2016-0213/CVE-2016-8388 描述了 Iceni Argus 中的任意堆覆盖漏洞。未经检查信任恶意字体内的索引使攻击者能够越界写入指定阵列外部。这可能导致以与本地用户相同的权限执行代码。

TALOS-2016-0214/CVE-2016-8389 描述了该工具尝试将 PDF 中的文本转换为多边形时发生的整数溢出。当应用尝试初始化多边形时，会越界写入因整数溢出而导致初始化大小太小的缓冲区外部。这可能导致在该工具尝试填充多边形时发生基于堆的缓冲区溢出。攻击者可以利用此漏洞，以与本地用户相同的权限执行代码。

Talos-2016-0228/CVE-2016-8715 涉及一个堆损坏漏洞，攻击者可利用该漏洞执行任意代码。如果经特殊设计的 PDF 文件包含设置为负数或大于特定值的 /Size 关键字，攻击者就可以写入堆中已经初始化的部分。攻击者可以利用此漏洞，以与本地用户相同的权限执行恶意代码。

TALOS-2017-0271/CVE-2017-2777 描述了 Iceni Argus 版本 6.6.05 中的堆溢出漏洞。经特殊设计的 PDF 文件可能导致整数溢出，进而导致在将该文件转换为 XHTML 时发生堆溢出。攻击者可以利用此漏洞，以与本地用户相同的权限执行代码。

防护

以下 Snort 规则可以检测此漏洞的漏洞攻击活动。请注意，Talos 未来可能会发布更多规则，当前的规则可能会根据可能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 FireSIGHT 管理中心或 Snort.org

Snort 规则：40917-40926、40872-40875、41327 和 41328

发布者：HOLGER UNTERBRINK；发布时间：0:59