2017 年 7 月 11 日，星期二

漏洞聚焦：Iceni Infix PDF 编辑器内存损坏漏洞

Talos 今天披露了一个在 Iceni Infix PDF 编辑器中发现的漏洞，该漏洞可能会导致受影响主机上发生任意代码执行。攻击者可以通过诱使用户打开经特殊设计的 PDF 文件，来利用该漏洞触发缺陷。Talos 团队已与 Iceni 进行协调，确保会公布与该漏洞相关的详细信息。Iceni 已通过相应的软件更新解决了此漏洞。此外，Talos 还制定了 Snort 规则，可用于检测尝试利用此缺陷的行为。

漏洞详细信息

TALOS-2017-0367 由 Talos 团队的 Piotr Bania 发现。

TALOS-2017-0367 (CVE-2017-2863) 是 Iceni Infix 中的内存损坏漏洞，攻击者可利用此漏洞在受影响的设备上实现任意代码执行。TALOS-2017-0367 的表现形式是在 PDF 解析功能中造成越界写入缺陷。如果用户打开经特殊设计的，以此漏洞为攻击目标的 PDF 文件，就有可能会遭到攻击。最可能的攻击形式是在社交工程场景下，用户收到包含恶意 PDF 的邮件，从而引发针对此漏洞的攻击。

有关更多技术详情，请阅读我们此处的公告。

防护

Talos 已开发以下 Snort 规则以检测试图利用此漏洞的攻击尝试。请注意，随着我们获得更多信息，这些规则会相应更新。如需获取最新信息，请访问您的 Firepower 管理中心或 Snort.org。

Snort 规则：43212-43213

如需了解 Talos 发现的其他漏洞，请参阅我们的漏洞报告门户网站：
http://www.talosintelligence.com/vulnerability-reports/

如需查看我们的漏洞披露政策，请访问以下站点：
http://www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html

发布者：NICK BIASINI 发布时间：10:29
标签：零日、ICENI、漏洞研究、漏洞聚焦