2016 年 10 月 18 日，星期二

漏洞聚焦：Foxit PDF 阅读器 JBIG2 解析器信息泄露漏洞

漏洞发现者：Talos 团队的 Aleksandar Nikolic。

Talos 发现 Foxit PDF 阅读器中存在信息泄露漏洞（TALOS-2016-0201/CVE-2016-8334）。Foxit PDF 阅读器在解析 PDF 中的 jbig2 片段时，会对“memcpy”执行含有边界错误的调用，导致越界堆内存被读取到缓冲区。由于“memcpy”调用采用正常大小，但源的大小却小于大小参数，所以会导致相邻内存被复制到缓冲区内。缓冲区内的堆元数据、地址和指针可能会被复制，并在以后被重复使用，导致内存布局泄漏。这个信息泄露漏洞连同另外一个漏洞一起，可能会被用于泄露堆内存布局和绕过 ASLR。网络钓鱼活动以 PDF 文件为载体（恶意附件或下载链接）散播恶意软件的情况很常见。

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：40429-40430

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/

发布者：WILLIAM LARGENT；发布时间：14:13
标签：零日、FOXIT、信息泄露、TALOS、漏洞研究、漏洞聚焦