2017 年 3 月 9 日，星期四

漏洞聚焦：R 语言 - PDF LoadEncoding 代码执行漏洞

漏洞发现者：思科 Talos 团队的 Cory Duplantis

概述

Talos 现披露 R 编程语言 3.3.0 版 LoadEncoding 功能中的缓冲区溢出漏洞 TALOS-2016-0227/CVE-2016-8714。R 编程语言通常用于统计计算，并由 R Foundation for Statistical Computing 提供支持。R 语言因拥有各种各样的统计和图形功能而受到赞誉。该漏洞具体与创建 PDF 文档相关。

详细信息

此漏洞具体影响到 R 语言的 PDF 创建功能。在创建 PDF 文档的过程中，用户可以指定包含编码阵列的文件。以下命令可以为 PDF 指定编码文件。

```
pdf(encoding="/path/to/some/file")
```

加载此文件时，文件中的每个特定元素都会被复制到“encnames”阵列中每个项目的“cname”元素中。“encnames”阵列是 EncodingInfo 结构的一部分。“encnames”阵列的结构类型为 'CNAME'，具有缓冲区长度设定为 40 的“cname”属性。如果提供的编码文件中有某个元素的长度大于 40，则会导致缓冲区溢出。攻击者有可能稍后在程序中利用此溢出远程执行代码。该漏洞的完整详细信息可在思科网站上的漏洞公告中找到。

防护

以下 Snort 规则可以检测相关的漏洞攻击活动。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：40894、40895

发布者：NICK BIASINI；发布时间：10:22
标签：零日、TALOS、漏洞研究、漏洞聚焦