2017 年 9 月 14 日，星期四

漏洞聚焦：Ansible-Vault 和 Tablib 中的 YAML 解析远程代码执行漏洞

漏洞发现者：Talos 团队的 Cory Duplantis。

Talos 现披露 Ansible-Vault 和 Tablib 的“另一种标记语言”(YAML) 处理过程中存在的远程代码执行漏洞。利用这些漏洞，攻击者可以通过发送恶意 YAML 内容在受影响的系统中执行任意命令。

概述

YAML 是一种数据序列化标记格式，这种语言既能被人工识别，又容易被计算机解析。目前，用于解析 YAML 数据的工具和库比比皆是。Python 的 YAML 解析库 PyYAML 提供了以下两种 API 调用方式，用于解析 YAML 数据：yaml.load 和 yaml.safe_load。其中，前一种 API 无法对 YAML 输入进行正确的净化，使得攻击者有机会在 YAML 内容中嵌入所要执行的 Python 代码。

如果应用包含 PyYAML 库，并且使用 yaml.load 调用方式（而非 yaml.safe_load），则有可能受到远程代码执行漏洞攻击。

TALOS-2017-0305 Ansible-Vault 库中的远程代码执行漏洞。(CVE-2017-2809)

Ansible 为自动执行 IT 任务和基于网络的任务提供了一种简单的解决方案。为了方便使用，它以 YAML 语言描述这些任务。Ansible-Vault 是一款第三方 Python 库，用于查看和修改 Ansible Vault 文件。此漏洞存在于该第三方库查看加密 Vault 文件的过程中。加载经过加密的 YAML 代码时，应用会调用不安全的 API 调用方式“yaml.load”。此漏洞可能导致恶意用于以当前用户身份远程执行任意代码。

该第三方 Python 库不同于 Ansible 提供的 Ansible-Vault 的核心功能，后者并不存在此漏洞。

有关更多技术详情，请参阅此 Talos 漏洞报告

TALOS-2017-0307 Tablib 中的远程代码执行漏洞。(CVE-2017-2810)

Tablib 是一种 Python 数据集库，可使各种程序轻松访问、写入和管理表格数据文件。该库已广泛用于各种应用，包括 django-import-export 应用。

Tablib 的数据表功能也包含调用不安全 API“yaml.load”的操作，而且该应用没有对用户提供的 YAML 代码进行适当的净化。恶意用户可以在数据表中嵌入恶意 YAML 代码，从而以当前用户身份远程执行任意代码。

有关更多技术详情，请参阅此 Talos 漏洞报告

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 将来可能会发布更多规则，当前规则会根据将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，请访问 FireSIGHT 管理中心或 Snort.org。

Snort 规则：42195-42196

特此感谢 Dylan Ayrey 在解决 TALOS-2017-0305 过程中提供的大力协助。

发布者：MARTIN LEE 发布时间：10:30 AM
标签：ANSIBLE VAULT、CVE-2017-2809、CVE-2017-2810、TABLIB、漏洞聚焦、YAML