2017 年 2 月 27 日，星期一

思科针对 Smart Install 客户端协议被滥用的保护措施

摘要

Talos 发现攻击者正在对客户基础设施进行频繁扫描，以期找到思科 Smart Install 客户端。思科 Smart Install 是促进 LAN 交换机管理的思科 Smart Operations 解决方案的一个组件。研究表明，有恶意攻击者可能正在利用对 Smart Install 协议的深入了解从受影响的设备获取客户配置副本。这种攻击利用 Smart Install 协议的一个已知问题。思科 PSIRT 已针对此活动发布了一个安全响应。滥用 Smart Install 协议可能导致修改 TFTP 服务器设置、通过 TFTP 窃取配置文件、更换 IOS 映像，甚至可能会执行 IOS 命令。

我们知道有一种公开发行的工具可用于扫描受影响的系统，该工具叫做 Smart Install Exploitation Tool (SIET)，可从此处获取。这个工具可能已被用于这些攻击。

保护

为了协助客户了解他们所面临的这个问题，我们发布了我们自己的扫描工具和可用来确定受影响的系统并检测 SIET 活动的初步 Snort 规则。

Talos 扫描实用程序

Talos 制作了一款扫描实用程序，所有用户都可以对自己的基础设施运行该实用程序以确定自己是否可能受到了 Smart Install 客户端协议被滥用的影响。该工具可以从此处获取。

防护

Snort 规则

Talos 以 SID 41722-41725 的形式创建了针对此问题的保护规则。这些规则随即会作为社区规则集的一部分公开发布，可从此处下载：

要获得保护，思科 FirePOWER 和 Snort 用户规则集客户应确保运行最新的规则更新。

此外，还可以使用通用 TFTP 活动规则 SID：518 和 SID：1444，但这些 SID 不是针对特定问题的，并且必须显式启用。

更多信息

点击以下链接即可查阅思科 PSIRT 就此问题发布的一篇博文：
https://blogs.cisco.com/security/cisco-psirt-mitigating-and-detecting-potential-abuse-of-cisco-smart-install-feature

点击以下链接即可查阅有关 Smart Install 安全实践的更多指导：
http://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/concepts.html#23355

点击以下链接即可查阅有关 Smart Install 的第三方研究信息：
https://2016.zeronights.ru/wp-content/uploads/2016/12/CiscoSmartInstall.v3.pdf

Talos 建议所有合作伙伴按照已发布的安全指南，快速采取措施保护自己的系统。

如果您遇到网络安全紧急情况，请拨打以下电话号码，与思科技术支持中心 (TAC) 联系：
在美国或加拿大境内，请拨打：+1 800 553-2447
在美国境外：请使用全球各地的相应联系方式

思科对正在进行的攻击响应迅速，可以与您的员工一起制定事件响应计划，尽可能降低当前和未来攻击的影响。

发布者：EARL CARTER；发布时间：16:42