预警编号：YJ-2018010

恒安嘉新

关于 Cisco Smart Install 远程命令执行

漏洞安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 4 月 07 日

1 漏洞描述

近期，互联网爆出 Cisco Smart Install 远程命令执行漏洞（CVE-2018-0171）。综合利用上述漏洞，允许未经身份验证的远程攻击者向远端 Cisco 设备的 TCP 4786 端口发送精心构造的恶意数据包，触发漏洞造成设备远程执行 Cisco 系统命令或拒绝服务（DoS）。目前，漏洞利用代码已公开，且厂商已发布漏洞修复版本。该漏洞危害程度为高危(High)。

2 影响范围

支持 Smart Install Client 模式的交换机受此漏洞影响，包括但不限于以下：

Catalyst 4500 Supervisor Engines

Catalyst 3850 Series

Catalyst 3750 Series

Catalyst 3650 Series

Catalyst 3560 Series

Catalyst 2960 Series

Catalyst 2975 Series

IE 2000

IE 3000

IE 3010

IE 4000

IE 5000

SM-ES2 SKUs

SM-ES3 SKUs

NME-16ES-1G-P

SM-X-ES3 SKUs

根据互联网数据显示，全球 Cisco Smart Install 系统规模约为 14.3 万；按国家分布情况来看，用户量排名前三的分别是美国（29%）、中国（11%）和日本（6%）。

3 漏洞原理

Smart Install 作为一项即插即用配置和镜像管理功能，为新加入网络的交换机提供零配置部署，实现了自动化初始配置和操作系统镜像加载的过程，同时还提供配置文件的备份功能。

Cisco Smart Install 存在远程命令执行漏洞，SMI IBC Server Process 进程中包含了 Smart Install Client 的实现代码。Smart Install Client 在 TCP（4786）端口上开启服务（默认开启），用来与 Smart Install Director 交互。当服务处理一段特殊构造的恶意信息 ibd_init_discovery_msg 时，因为未能检查拷贝到固定大小缓冲区的数据尺寸，大小和数据是直接从网络数据包中获得的，并由攻击者控制，smi_ibc_handle_ibd_init_discovery_msg 函数在处理该数据包时会触发缓冲区栈溢出造成设备拒绝服务（DoS）或远程执行 Cisco 系统命令。

4 修复建议

处置建议：

远程自查方法 A：

确认目标设备是否开启 4786/TCP 端口，如果开启则表示可能受到影响。

比如用 nmap 扫描目标设备端口：

nmap -p T:4786 192.168.1.254

远程自查方法 B：

使用 Cisco 提供的脚本探测是否开放 Cisco Smart Install 协议，若开启则可能受到影响。

pythonsmi_check.py -i 192.168.1.254

本地自查方法 A：（需登录设备）

此外，可以通过以下命令确认是否开启 Smart Install Client 功能：

switch>show vstack config

Role:Client (SmartInstall enabled)

Vstack Director IP address: 0.0.0.0

switch>show tcp brief all

TCB Local Address Foreign Address (state)

0344B794 *.4786 *.* LISTEN

0350A018 *.443 *.* LISTEN

03293634 *.443 *.* LISTEN

03292D9C *.80 *.* LISTEN

03292504*.80 *.* LISTEN

本地自查方法 B：（需登录设备）

switch>show version

将回显内容保存在 a.txt 中，并上传至 Cisco 的 Cisco IOS Software Checker 进行检测。

检测地址：https://tools.cisco.com/security/center/softwarechecker.x

修复方法：

升级补丁：

思科官方已发布针对此漏洞的补丁但未提供下载链接，详细修复方案如下：

临时处置措施：(关闭协议)

switch#conf t

switch(config)#no vstack

switch(config)#do wr

switch(config)#exit

检查端口已经关掉：

switch>show tcp brief all

TCB Local Address Foreign Address (state)

0350A018 *.443 *.* LISTEN

03293634 *.443 *.* LISTEN

03292D9C *.80 *.* LISTEN

03292504*.80 *.* LISTEN