Cisco IOS 与 IOS XE Software Smart Install 远程命令执漏洞（CVE-2018-0171）通告

文档信息

编号	360TI-SV-2018-008
关键字	CVE-2018-0171 Cisco Smart Install
发布日期	2018 年 3 月 30 日
更新日期	2018 年 4 月 7 日
TLP	WHITE
分析团队	360 威胁情报中心

通告背景

2018 年 3 月 28 日，Cisco 发布了一个远程代码执行严重漏洞通告。通告了思科 IOS 和 IOS-XE 系统的配置管理类协议 Cisco Smart Install（Cisco 私有协议）代码中存在一处缓冲区栈溢出漏洞，漏洞编号为 CVE-2018-0171。攻击者无需用户验证即可向远端 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）。

漏洞相关的技术细节和验证程序已经公开，且互联网上受影响的主机数量非常大。由于此漏洞影响底层网络设备，且漏洞相关 PoC 已经公开并证实可用，极有可能构成巨大的现实威胁。2018 年 4 月 7 日凌晨有 IDC 运营商报告有大量 Cisco 遭到利用此漏洞的攻击，导致设备配置被清空的情况， 360 威胁情报中心再次更新此通告提醒用户和企业尽快采取必要防御应对措施以保证网络的可用性。

漏洞概要

漏洞名称	Cisco IOS 与 IOS XE Software Smart Install 远程命令执行漏洞				
威胁类型	远程代码执行	**威胁等级**	高	**漏洞 ID**	CVE-2018-0171
漏洞利用条件					
开启了 Cisco Smart Install 管理协议，且模式为 client 模式					
漏洞利用场景					
攻击者无需用户验证即可向远端 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）。					
服务是否默认开启	是				
受影响系统及应用版本					
确认受影响的型号： Catalyst 4500 Supervisor Engines Cisco Catalyst 3850 Series Switches					

Cisco Catalyst 2960 Series Switches 可能受影响的设备型号： 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 4010 IE 5000 SM-ES2 SKUs SM-ES3 SKUs NME-16ES-1G-P SM-X-ES3 SKUs
不受影响影响系统及应用版本
未开启 Cisco Smart Install 管理协议或模式为 Director 模式的 Cisco 设备均不受影响。

漏洞描述

该漏洞存在于思科 IOS 和 IOS-XE 系统的配置管理类协议 Cisco Smart Install 一处缓冲区栈内。攻击者无需认证，远程向开启 TCP 4786 且为 client 模式的 Cisco 设备端口发送精心构造的畸形数据包，会导致 smi_ibc_handle_ibd_init_discovery_msg 函数在处理该数据包时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。

影响面评估

360 威胁情报中心已经确认公开的 PoC 利用代码有效，且该漏洞整体影响面非常大，综合分析威胁等级为高。

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。

```
# python smi_check.py -i 192.168.1.254
[INFO] Sending TCP probe to targetip:4786
[INFO] Smart Install Client feature active on targetip:4786
[INFO] targetip is affected。
```

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，请联系思科获取补丁。

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

参考资料

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2#fixed
https://embedi.com/blog/cisco-smart-install-remote-code-execution/

更新历史

时间	内容
2018 年 3 月 28 日	初始报告
2018 年 3 月 29 日	补充内容
2018 年 3 月 30 日	公开发布安全通告
2018 年 4 月 7 日	加入已经出现的现实利用攻击情况