天融信关于 Cisco Smart Install 远程代码执行漏洞的预警

天融信安全云服务运营中心

一、漏洞描述

1.1 漏洞背景

近日思科官方确认在 Cisco IOS 和 Cisco IOS-XE 系统的 Smart Install Client 组件中存在一处缓冲区溢出漏洞。该组件网络数据处理函数不严谨，数据和数据长度均直接从网络数据包中获取，因为未检查复制到固定大小缓冲区的数据长度，造成了缓冲区溢出漏洞。该漏洞编号为： CVE-2018-0171。漏洞使得攻击者无需身份验证即可远程执行任意代码，因此攻击者可以完全控制存在漏洞的网络设备。

1.2 漏洞影响

该漏洞已确认影响以下设备：

Catalyst 4500 Supervisor Engines
Cisco Catalyst 3850 Series Switches
Cisco Catalyst 2960 Series Switches

部分属于 Smart Install Client 类型的设备可能同样受到该漏洞的影响，列表如下：

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 4010
IE 5000
SM-ES2 SKUs
SM-ES3 SKUs
NME-16ES-1G-P
SM-X-ES3 SKUs

二、检测及修复建议

2.1 检测是否存在漏洞

确认思科网络设备是否开启 TCP 4786 端口，一旦开启该端口， 则可能存在漏洞。比如使用如下 nmap 命令扫描思科网络设备：

```
nmap -p T:4786 192.168.1.0/24
```

还可以使用如下命令确认您的设备是否为 Smart Install Client 类型，如果属于该类型设备则可能存在漏洞，命令如下：

```
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
```

2.2 临时措施（关闭协议）

```
switch#conf t
switch(config)#no vstack
switch(config)#do wr
switch(config)#exit
```

2.3 其他建议

官方暂无修补方案，更多信息您可以关注思科官方网站

Cisco Security Advisory：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2#fixed

Cisco Feature Navigator：

http://cfn.cloudapps.cisco.com/ITDIT/CFN/jsp/index.jsp

Supported Devices for Smart Install：

https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/supported_devices.html#51890