computer emergency response team CERT-EU for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2018-009

Cisco Smart Install Protocol Remote Code Execution Vulnerability

April 10, 2018 — v1.1

History:

- *06/04/2018 — v1.0 – Initial publication*
- *10/04/2018 — v1.1 – Additional information added*

Summary

On 28th of March 2018, Cisco published a security advisory concerning a buffer overflow discovered in Smart Install feature of Cisco IOS and Cisco IOS XE software. This vulnerability allows an unauthenticated, remote attacker to execute arbitrary code on an affected device [1].

Successful exploitation may lead to:

- triggering a reload of the device,
- executing arbitrary code on the device,
- causing an indefinite loop on the affected device that triggers a watchdog crash.

This vulnerability has been assigned the number CVE-2018-0171.

According to the researchers which originally reported the vulnerability, this is a **critical vulnerability** [2]:

```
AV:N/AC:L/Au:N/C:C/I:C/A:C (10.0).
```

A proof of concept for the vulnerability has been published [2]. As of the time of this writing, there are about 168 000 vulnerable devices accessible on the Internet according to Shodan. Also, there are already many attacks observed in the wild.

A patch for this vulnerability was released as part of the March 28, 2018, *Cisco IOS and IOS XE Software Security Advisory Bundled Publication*, which includes 20 Cisco security advisories that describe 22 vulnerabilities [1].

Cisco devices that are configured as a *Smart Install Director* are not affected by these attacks.

Products Affected

According to Cisco Advisory [1], this vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS or IOS XE software and have the Smart Install Client feature enabled.

Only Smart Install Client switches are affected by the vulnerability that is described in this advisory. Cisco devices that are configured as a Smart Install Director are not affected (see the details about the components of the Smart Install Network below).

Smart Install Client functionality is enabled by default on Cisco IOS switches on software releases that have not been updated to address Cisco bug ID `CSCvd36820`.

Cisco has published a list of devices supporting Smart Install [3].

Technical Details

According the original research, which won the G-Influence award at GeekPWN 2017 Hong-Kong after its successful exploitation had been demonstrated [2], the Smart Install Client starts a server on the TCP(4786) port (open by default) to interact with the Smart Install Director.

When the server is processing a specially crafted malicious message, a stack-based buffer overflow occurs because the size of the data copied to a fixed-size buffer is not checked. The size and data are taken directly from the network packet and could be controlled by an attacker.

Some details on the techniques and methods used to create the exploit for this vulnerability can be found in the research *How To Cook Cisco* from the original reporter [5].

Main Components of the Smart Install Network

The *Director* builds a topology database for the network by collecting information from the network Smart Install switches.

The Director uses the database:

- to assign a configuration file and image to a client,
- as a reference to obtain the PID, the image name, and the configuration file for an on-demand update of network switches.

Smart Install network uses DHCP server to assign IP addresses for transfer of specific parameters. It also relies on a TFTP server to store image and configuration files. The TFTP server can be an external device, or the Director can act as a TFTP server. Client switches have a direct or indirect connection to the Director so that they can receive image and configuration downloads from it.

More information about the Smart Install technology can be found in the official documentation [4].

Recommendations

Follow these general steps in order to fix this vulnerability:

- determine whether the Smart Install Client feature is enabled,
- determine the Cisco IOS or the Cisco IOS XE software version,
- fix the vulnerability thorough the upgrading procedures or support contact.

The detailed instructions for each of the above points are available in the original Cisco Security Advisory [1].

Workarounds

If – for any reason – it was not possible to apply the proper patch made available by Cisco, these are some possible mitigating actions to consider:

Disabling the Smart Install Client Functionality

As previously mentioned, this feature might be active or not by default, depending on the software version and the patches applied. It is important to follow the official documentation for the specific software release to accomplish this task. In addition, some sources claim that this configuration could be reset after reboot, depending on the software version and the patches applied [7, 8].

Limiting Access

If this functionality is required and the patch cannot be applied, it might be useful to introduce access-lists in the router to limit the IPs allowed to access this facility. Some examples can be found in [8], but it is always better to refer the official guide for the specific software release.

It also advisable to block this service on the perimeter firewall, and possibly consider using a VPN if this service is required to be available from outside of the organization.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

[2] https://embedi.com/blog/cisco-smart-install-remote-code-execution/

[3] https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/supported_devices.html

[4] https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/concepts.html

[5] https://embedi.com/blog/how-cook-cisco/

[6] https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/commands.html

[7] https://www.kaspersky.com/blog/cisco-apocalypse/21966/

[8] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi