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

CERT-EU Security Advisory 2017-003

Cisco Smart Install Protocol Issues

February 22, 2017 — v1.0

History:

- *22/02/2017 — v1.0 – Initial publication*

Summary

Several researchers (e.g., in [4]) and CERT/CSIRTs have reported on the misuse of Cisco Smart Install (SMI) [1] protocol messages. The misuse is directed towards ***Smart Install Clients*** allowing an unauthenticated remote attacker to:

- obtain and change the startup-config file and force a reload of the device,
- load a new IOS image on the device, and execute high-privilege CLI commands on switches running Cisco IOS and IOS XE Software.

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

Cisco does not consider this issue a vulnerability in Cisco IOS, IOS XE, or the Smart Install feature itself, but a **misuse** of the Smart Install protocol, which does not require authentication by design. However, since Cisco Smart Install (SMI) is enabled by default in a big number of modern switches and routers, CERT-EU considers this protocol abuse a potentially **serious threat**.

Technical Details

Smart Install is a *plug-and-play* configuration and image-management feature that provides zero-touch deployment for new switches. The Smart Install feature incorporates no authentication by design.

SmartInstall also has mechanisms in place for subsequent Cisco IOS Software and configuration upgrades on groups of switches, using a single command line interface (CLI) and switch replacement assistance. It can perform a configuration backup when a switch changes its configuration.

A Smart Install network consists of exactly one *Smart Install Director* switch or router, also known as an *integrated branch director* (IBD), and one or more *Smart Install Client* switches, also known as *integrated branch clients* (IBCs). A client switch does not need to be directly connected to the director but can be up to seven hops away.

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.

Smart Install 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.

Issues Identified

Knowing the characteristics of the protocol, the researchers have managed to [4]:

- Change the TFTP server address on a client device by sending one malformed TCP packet.
- Copy client's startup-config to the new TFTP server.
- Substitute client's startup-config with another, manually modified one. Client device will then reboot at predefined time.
- Upgrade IOS image on the client device.
- Execute random set of commands on the client device (it is a new feature working only at 3.6.0E and 15.2(2)E IOS versions).

A proof of concept is available [5].

Products Affected

An extensive list (50+) of affected switches and routers can be found in [3].

Recommendations

- Cisco has updated the Smart Install Description chapter in the *Cisco Smart Install Configuration Guide* [2] to include *Security Best Practices* when deploying Cisco Smart Install functionality.
- The protocol does not require authentication by design, and the suggested best practices should be applied depending on how the feature is used in a specific customer environment.
- Organizations that are not leveraging the Smart Install feature, or using it purely for zero-touch deployment, should disable the Smart Install feature once the switch has been deployed with the configuration command `no vstack`.

- Where the `no vstack` command is not available (old versions), organizations should ensure that only the IB Director has TCP connectivity to all IB Clients on port 4786, by using:
  - interface access control lists (ACLs),
  - Control Plane Policing (CoPP is not available on all Cisco IOS Software releases).
- Organizations that are seeking more than just zero-touch deployment, or need the added security of authorization and authentication between the director and clients, can migrate to Cisco Plug-N-Play (PnP).
- Segment the network into multiple zones focusing specifically on separating the management network segment.

Mitigations Summary

Use Case	**Mitigation**
- Customers not using the Smart Install feature.	- Disable (`no vstack`).
- Customers leveraging the Smart Install feature only for zero-touch deployment.	- Disable (`no vstack`) after initial deployment.
- Customers leveraging the Smart Install feature for more than zero-touch deployment (configuration and image-management). - Customers running old versions.	- Interface access control lists (ACLs). - Control Plane Policing (CoPP).

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20170214-smi

[2] http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-x-series-switches/white_paper_c11-651895.html

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

[4] https://2016.zeronights.ru/wp-content/uploads/2016/12/CiscoSmartInstall.v3.pdf

[5] https://github.com/Sab0tag3d/SIET