NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

CISCO®[1] SMART INSTALL PROTOCOL MISUSE

BLUF: Disable the Smart Install auto-loading feature on all network devices.

PURPOSE:

Adversaries are likely exfiltrating copies of configuration files on internet accessible switches using the Cisco Smart Install functionality. This protocol exposes infrastructure devices to increased operational risk, which could compromise device integrity. Malicious Smart Install protocol messages can allow an unauthenticated, remote attacker to change the startup-config file, 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.

OPERATIONAL SECURITY CONCERN:

These configuration files allow an adversary to map and move laterally through the network. An adversary can also deploy modified IOS images and configuration changes to the switches. A maliciously crafted IOS or altered configuration file will allow an adversary to further compromise the network. It is important to note that this feature is enabled by default on supported IOS images.

DETECTION:

- Examine the output of “*show vstack config* | *inc Role*”. The presence of “Role: Client (SmartInstall enabled)” indicates that Smart Install is configured.

- Examine the output of "**show tcp brief all**" and look for "*:**4786**". The Cisco Smart Install feature listens on **tcp/4786.**

  Note: The commands above will indicate if the feature is enabled on the device and not that a device has been compromised.

MITIGATION ACTIONS:

- Per DISA STIG rule: SV-3080r3_rule, configuration auto-loading feature must be disabled. Therefore, Smart Install must be disabled on all Cisco switches. The command “***no vstack***” will disable the feature.

- Review all Cisco switch configuration files for deviations from documented pre-existing configurations.

- If a deny-by-default strategy is not already implemented at edge firewall devices, the layer-7 TFTP application, port udp/69, and port tcp/4786 must be denied.

[1] Cisco® and Cisco IOS® are registered trademarks of Cisco Systems, Inc.

REFERENCES:

DISA STIG NET0760 SV-3080r3_rule: *The Configuration auto-loading feature must be disabled* (28 April 2017)

CISCO PISRT CISCO-sr-20170214-smi: Cisco Smart Install Protocol Misuse (14 February 2017)

DISCLAIMER OF WARRANTIES AND ENDORSEMENT:

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

FOR FURTHER INFORMATION, PLEASE CONTACT:

Client Requirements or General Cybersecurity Inquiries
Cybersecurity Requirements Center
410-854-4200
email: Cybersecurity_Requests@nsa.gov