NATIONAL SECURITY AGENCY
CYBERSECURITY OPERATIONAL RISK NOTICE

MULTIPLE CRITICAL VULNERABILITIES IDENTIFIED IN CISCO SMART INSTALL

RISK

This notice is to inform customers, partners, stakeholders and the general community of ongoing exposure to a known vulnerability despite vendor released patches, fixes, and guidance. Exploits for this vulnerability are publicly available and adversarial intent and usage is currently observed in the wild.

On 28 March 2018, Cisco®[1] released two new vulnerabilities in their proprietary Smart Install feature that allow a remote attacker to achieve remote code execution and Denial of Service conditions. The DODIN is currently blocking all Smart Install traffic (port 4786) at the network edge; however, any devices within the DODIN that have not disabled Smart Install are now vulnerable to remote code execution through lateral movement. This threat leaves the DODIN vulnerable to internal threats and lateral expansions from adversaries that achieve access within the DODIN borders.

VULNERABILITY DISCUSSION

The first vulnerability released by Cisco is an unauthenticated remote code execution vulnerability that ranked as a 9.8 on the common vulnerability scoring system (CVSS) scale. This identifies the vulnerability as CRITICAL and requires immediate remediation. The vulnerability is due to improper validation of packet data allowing an attacker to send a crafted Smart Install message to an affected device on TCP port 4786 causing one of the following impacts:

- Trigger a reload of the device
- Allow the attacker to execute arbitrary code on the device
- Cause an indefinite loop on the affected device that triggers a watchdog crash

The second vulnerability released by Cisco is an unauthenticated denial of service attack that ranked as an 8.6 on the CVSS scale. This identifies the vulnerability as HIGH and should be remediated immediately. The vulnerability is also due to improper validation of a crafted Smart Install packet that can cause the device trigger a reboot. Repeatedly sending these specially crafted Smart Install packets can lead to infinite reboots rendering the device unavailable.

Products currently vulnerable to both of these vulnerabilities include all Cisco IOS®[2] and IOS XE devices that have Smart Install enabled and have not installed the software updates to address Cisco bug ID CSCvd36820.

VULNERABILITY PREVALENCE & IMPACT FROM EXPLOITATION

An online vulnerability scanning service known as Shadow Server is currently reporting over 49,000 devices in the United States that are currently listening for Smart Install on the Internet. This feature is enabled by default all IOS and IOS XE devices running software after version 12.2(52)SE and are vulnerable.

[1] Cisco is a registered trademark of Cisco Systems, Inc.

[2] Cisco IOS is a registered trademark of Cisco Systems, Inc.

VULNERABILITY DETECTION ACTIONS

To detect if a devices is vulnerable to these vulnerabilities, follow the steps below on all Cisco IOS and IOS XE devices:

- Examine the output of “show version”. If the current version of software is above 12.2(52)SE then continue to determine status of Smart Install.
- 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.

REMEDIATION REQUIREMENTS & ADVISORIES

- 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)
- Information Assurance Advisory IAA U/OO/801020-17: Cisco Smart Install Protocol Misuse (7 August 2017)

MITIGATION ACTIONS

- Utilize the Cisco IOS Software Checker tool to identify the patched software for Cisco bug IDs CSCvd40673 and CSCvd76186 and upgrade to patched software.
- 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, port tcp/4786 must be denied.

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.

CONTACT INFORMATION

Client Requirements and General Cybersecurity Inquiries:

Cybersecurity Requirements Center
410-854-4200
Email: Cybersecurity_Requests@nsa.gov