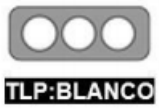

CISCO SMART INSTALL

1. INTRODUCCIÓN

Cisco Smart Install - SMI es una función de imágenes, configuración y administración «plug-and-play» del fabricante CISCO, que permite a las organizaciones incorporar nuevos dispositivos de comunicaciones a la red sin la necesidad o con una mínima intervención de una persona para configurarlos y de esta manera inicien sus operaciones. La simple conexión a la red del dispositivo hace que este se auto configure con base a la información transmitida por otro dispositivo de capa 3 ya existente en la red.

La función Smart Install no incorpora autenticación por diseño, por tal motivo, un atacante remoto no autenticado podría cambiar el archivo de configuración de inicio, forzar un reinicio del dispositivo, cargar una nueva imagen del sistema operativo y ejecutar comandos CLIs privilegiados, es decir tomar el control total del dispositivo y usarlo para actividades maliciosas.

2. RIESGO

Los dispositivos de comunicaciones en los que se encuentre habilitada la funcionalidad Cisco Smart Install con configuración de fábrica y que no se ha implementado un mecanismo de control de acceso, permite la explotación de la configuración por defecto, esto puede generar los siguientes escenarios:

- Acceso no autorizado a los archivos de configuración que contienen entre otros datos la contraseña de administración del dispositivo.
- Modificación de los parámetros de operación del dispositivo, impactando a la confidencialidad, integridad y disponibilidad de la información, y servicios gestionados por el dispositivo comprometido.
- Creación no autorizada de perfiles de usuario con privilegios de administración, con lo que se toma el control total del dispositivo.

3. DETECCIÓN

Para identificar si un dispositivo tiene habilitado el servicio SMI, se debe ejecutar el comando “show vstack config”, que mostrará si el servicio se encuentra activo en el dispositivo y es un cliente sujeto a recibir paquetes de configuración Cisco SMI que lo haría vulnerable.

4. ACCIONES RECOMENDADAS.

- Una vez que el nuevo dispositivo se instale en la red, el administrador debe deshabilitar la opción Cisco Smart Install para lo cual debe ejecutar el comando “no vstack”.
- En los casos en que no se pueda ejecutar el comando “no vstack”, se deberán implementar controles de acceso a fin de que solo el dispositivo director tenga conexión TCP al puerto 4786 hacia los nuevos dispositivos a conectarse en la red.

5. REFERENCIAS

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi
https://smartinstallscan.shadowserver.org/