Investigadores descubrieron una grave vulnerabilidad en productos Cisco que permite a los hackers implantar backdoors persistentes en dispositivos de amplio rango utilizados en empresas y redes gubernamentales, incluidos enrutadores, conmutadores y cortafuegos.

Apodada como Thrangrycat, □□□ , la vulnerabilidad, descubierta por investigadores de la compañía de seguridad Red Balloon, e identificada como CVE-2019-1649, afecta a distintos productos de Cisco que admiten el módulo Trust Anchos (TAm).

El módulo Trust Anchor es una funcionalidad de inicio seguro basada en hardware implementada en la mayoría de los dispositivos empresariales de Cisco desde 2013 que garantiza que el firmware que se ejecuta en las plataformas de hardware sea auténtico y no haya sido modificado.

Sin embargo, los investigadores encontraron una serie de fallas en el diseño del hardware que permitiría que un atacante autenticado realice la modificación persistente del módulo Trust Anchor por medio de la modificación del flujo de bits FPGA y cargue el bootloader malicioso.

> *«Un atacante con privilegios de root en el dispositivo puede modificar el contenido del flujo de bits de anclaje FPGA, que se almacena sin protección en la memoria flash. Los elementos de este flujo de bits se pueden modificar para deshabilitar la funcionalidad crítica en el TAm»,* dijeron los investigadores.
>
> *«La modificación exitosa del flujo de bits es persistente, y el Trust Anchor se desactivará en las siguientes secuencias de arranque. También es posible bloquear cualquier actualización de software al flujo de bits de TAm».*

Encadenamiento con errores remotos: no se requiere acceso físico

Dado que la explotación de la vulnerabilidad requiere privilegios de root, un aviso publicado

por Cisco destacó que solo un atacante local con acceso físico al sistema de destino podría escribir una imagen de firmware modificada en el componente.

Sin embargo, los investigadores de Red Balloon explicaron que los atacantes también podrían explotar dicha vulnerabilidad de Thrangrycat de forma remota encadenándola con otras fallas que podrían permitirles obtener acceso root o, al menos, ejecutar comandos como root.

Para demostrar este ataque, los investigadores revelaron una vulnerabilidad de RCE (CVE-2019-1862) en la interfaz de usuario basada en la web del sistema operativo IOS de Cisco que permite a un administrador registrado ejecutar comandos arbitrarios en el shell de Linux subyacente de un dispositivo afectado con privilegios de root.

Después de obtener acceso root, el administrador malintencionado puede omitir remotamente el módulo Trust Anchor en un dispositivo específico utilizando la vulnerabilidad de Thrangrycat e instalar una puerta trasera maliciosa.

> *«Al encadenar □□□ y las vulnerabilidades de inyección remota de comandos, un atacante puede omitir de forma remota y persistente el mecanismo de arranque seguro de Cisco y bloquear todas las futuras actualizaciones de software para el TAm. Dado que las fallas residen en el diseño del hardware, es poco probable que cualquier parche de seguridad del software resuelva completamente la vulnerabilidad de seguridad fundamental»,* dijeron los investigadores.

Mientras los investigadores probaron las vulnerabilidades contra los enrutadores Cisco ASR 1001-X, cientos de millones de unidades de Cisco que ejecutan un TAm basado en FPGA en todo el mundo, que incluye todo desde enrutadores empresariales hasta conmutadores de red y cortafuegos, son vulnerables.

Red Balloon Security informó los problemas a Cisco de forma privada en noviembre de 2018 y solo publicó algunos detalles al público luego de que Cisco emitió parches de firmware para solucionar ambos defectos, además de enumerar todos los productos afectados.

Cisco dijo que la compañía no detectó ataques que explotaran ninguna de las dos vulnerabilidades.

Los detalles completos de la vulnerabilidad serán publicados en la conferencia de seguridad Black Hat USA de este año, en agosto.