Se encontró que varios equipos de red fabricados por Cisco son vulnerables a cinco nuevas vulnerabilidades de seguridad que podrían permitir a los hackers tomar el control total sobre ellos, y luego, sobre las redes empresariales que alimentan.

Cuatro de los cinco errores de alta gravedad son problemas de ejecución remota de código que afectan a los enrutadores, conmutadores y cámaras IP de Cisco, mientras que la quinta vulnerabilidad es un problema de denegación de servicio que afecta a los teléfonos IP de Cisco.

Se denominó colectivamente a las vulnerabilidades como «CDPwn», que residen en las diversas implementaciones del Cisco Delivery Protocol (CDP) que viene habilitado de forma predeterminada en casi todos los dispositivos Cisco y no se puede apagar.

Cisco Delivery Protocol es un protocolo administrativo que funciona en la capa 2 de la pila de Protocolo de Internet (IP). El protocolo ha sido diseñado para permitir que los dispositivos descubran información sobre otros equipos Cisco conectados localmente en la misma red.

Según un informe que el equipo de investigación de Armis compartió con THN, las implementaciones de CDP subyacentes contienen desbordamiento de búfer y vulnerabilidades de cadena de formato que podrían permitir a los atacantes remotos en la misma red ejecutar código arbitrario en los dispositivos vulnerables mediante el envío de paquetes CDP maliciosos no autenticados.

La lista de vulnerabilidades de Cisco CDPwn que afectan a decenas de millones de dispositivos ampliamente implementados en redes empresariales es la siguientes:

- Cisco NX-OS Stack Overflow en el Power Request TLV (CVE-2020-3119)
- Vulnerabilidad de cadena de formato Cisco IOS XR en múltiples TLV (CVE-2020-3118)
- Cisco IP Phones Stack Overflow en PortID TLV (CVE-2020-3111)
- Desbordamiento de cámaras IP de Cisco en DeviceID TLV (CVE-2020-3110)
- Agotamiento de recursos de Cisco FXOS, IOS, XR y NX-OS en las direcciones TLV (CVE-2020-3120)

Cabe mencionar que, debido a que CDP es un protocolo de capa 2 de enlace de datos que no puede cruzar los límites de una red de área local, un atacante primero debe estar en la misma red para aprovechar las vulnerabilidades de CDPwn.

Sin embargo, luego de obtener un punto de apoyo inicial en una red objetivo utilizando vulnerabilidades separadas, los hackers pueden ser capaces de explotar CDPwn contra los conmutadores de red para romper la segmentación de la red y moverse lateralmente por medio de las redes corporativas a otros sistemas y datos sensibles.

> *«Obtener el control sobre el conmutador es útil de otras formas. Por ejemplo, el conmutador está en una posición privilegiada para espiar el tráfico de red que atraviesa el conmutador, e incluso se puede usar para lanzar ataques de intermediario en el tráfico de dispositivos que atraviesa el interruptor»*, dicen los investigadores.
>
> *«Un atacante puede mirar para moverse lateralmente por medio de segmentos y obtener acceso a dispositivos valiosos como teléfonos IP o cámaras. A diferencia de los interruptores, estos dispositivos contienen datos sensibles directamente, y la razón para tomarlos puede ser el objetivo de un atacante, y no simplemente una forma de salir de la segmentación».*

Además, las vulnerabilidades de CDPwn también permiten a los atacantes:

- Escuchar los datos o llamadas de voz y video, y la transmisión de video de teléfonos IP y cámaras, además de capturar conversaciones o imágenes sensibles.
- Extraer datos corporativos confidenciales que fluyan por medio de los conmutadores y enrutadores de la red corporativa.
- Comprometer los dispositivos adicionales al aprovechar los ataques man-in-the-middle para interceptar y alterar el tráfico en el conmutador corporativo.

Además de publicar un informe técnico detallado acerca de los problemas, el equipo de investigación de Armis también compartió videos de explicación y demostración de las fallas, como se incluyó anteriormente.

Luego de trabajar estrechamente con los investigadores de Armis en los últimos meses para desarrollar parches de seguridad, Cisco lanzó hoy actualizaciones de software para todos sus productos afectados.

Aunque Cisco también proporcionó información de mitigación, los administradores afectados deberían instalar las últimas actualizaciones de software para proteger completamente sus redes.