


**Accesible CWMP**

(CWMP: CPE WAN Management Protocol)

## 1. INTRODUCCIÓN

CWMP es un protocolo de capa de aplicación para la **administración remota de equipos locales del cliente** (Customer Premises Equipment CPE) conectado a una red de Protocolo de Internet (IP).

La administración del protocolo se dirige al creciente número de dispositivos de acceso a Internet como módems, enrutadores, puertas de enlace, así como a dispositivos de usuario final que se conectan a Internet, como decodificadores y teléfonos VoIP.

CWMP es un protocolo cuyo puerto asignado es el 7547. Algunos dispositivos utilizan el puerto 30005.

## 2. RIESGO

La explotación de esta vulnerabilidad permitiría a un atacante tomar control de dispositivos conectados a Internet, con capacidad para robar datos personales y financieros de consumidores y empresas e incluso la interrupción de los servicios de Internet de la empresa/usuario que se vea afectada.

## 3. DETECCIÓN

Para verificar manualmente si el sistema de uno de los dispositivos CPE es vulnerable, se puede utilizar el siguiente comando desde el internet o desde la red interna, dependiendo de la ubicación del CPE:

sudo nmap –sT –p &port &ip_addr

Donde:

| Argumento | Explicación |
|---|---|
| nmap: | Comando para ejecución de Nmap |
| -sT | Determina TCP |
| -p | Selecciona el puerto |
| IP | La dirección IP del sistema a verificar |

| | |
|---|---|
| 5353 | Puerto 5353 por el cual se enviara la respuesta del servicio |

**Ejemplo:**

Desde Internet
sudo nmap –sT –p 7547 181.199.xxx.xxxx
sudo nmap –sT –p 30005 66.125.xxx.xxx
Desde Red interna
sudo nmap –sT –p 7547 10.10.xxx.xxx
sudo nmap –sT 30005 172.168.xxx.xxx

## 4. ACCIONES RECOMENDADAS

- Es recomendado el uso de TLS para transportar el protocolo CPE WAN Management Protocol CWMP. TLS proporciona confidencialidad e integridad de datos y permite la autenticación basada en certificados en lugar de la autenticación compartida basada en secretos.

- En caso de no usar la funcinalidad proporcionada por CWMP, factor bloquee los puertos 7547, 30005 y no exponga los detalles de configuración del protocolo CWMP.

## 5. REFERENCIAS

- http://www.freeacs.com/
- https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763
- http://www.conectronica.com/wireless/redes-wireless/tr-069-y-la-gestion-de-miles-de-millones-de-dispositivos
- https://www.qacafe.com/training/best-practices-for-securing-tr-069/
- https://www.shadowserver.org/what-we-do/network-reporting/open-cwmp-report/