[TLP BLANCO]: La información podrá ser compartida libremente de acuerdo con las reglas y procedimientos aplicables para la divulgación pública Debe regirse a las normas estándar de derechos de autor.

Open-SSDP (Simple Service Discovery Protocol)

1. INTRODUCCIÓN

SSDP es un protocolo que sirve para la búsqueda de dispositivos UPnP en una red. Utiliza UDP en unicast o multicast en el puerto 1900 para anunciar los servicios de un dispositivo. En los mensajes intercambiados se envía la información acerca el dispositivo y el servicio ofrecido.

SSDP permite que los dispositivos conectados a una red descubran ciertos servicios contactables como impresoras y servidores, también permite que otros dispositivos en la red detecten nuevos nodos.

Ciertos protocolos UDP envían respuestas a ciertos comandos con paquetes de información que son más grandes que la petición inicial; es decir, un solo paquete puede generar decenas o cientos de veces el ancho de banda original en su respuesta (ataque de amplificación).

Algunos protocolos UDP, y sus factores de amplificación de ancho de banda, que han sido identificados como posibles vectores de ataque se enumeran a continuación:

Protocolos UDP	Bandwidth Amplification Factor (BAF)
DNS	28 a 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	**30.8**
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5

Fuente: https://www.us-cert.gov/ncas/alerts/TA14-017A

2. RIESGO

UDP, es un protocolo no orientado a conexión que no valida las direcciones IP de origen, a menos que el protocolo de capa de aplicación utilice mecanismos de inicio de sesión. Cuando el paquete UDP tiene la dirección IP de origen falsificada (victima), el servidor responde a la víctima, creando un ataque de Denegación reflejada de servicio (RDoS).

Un ataque DRDOS (*Distributed Reflective Denial of Service*) es una forma de ataque DDoS (*Distributed Denial of Service*) que se basa en el uso de servidores UDP de acceso público y usa BAF para congestionar a un sistema víctima con tráfico UDP. El atacante suplanta la IP de la víctima y envía muchas solicitudes al servidor, el tamaño de las respuestas van a ser mayores que las solicitudes, quien las recibe va a ser la víctima y no el atacante, la victima recibe inundaciones con tráfico no deseado, ataque DDoS

3. DETECCIÓN

El reporte de “Open SSDP” se basa en peticiones UDP al puerto 1900 de servidores con direcciones IPv4, si SSDP está habilitado a internet como respuesta se verá información SSDP.

La comprobación se realiza usando los siguientes comandos en Linux:

- Ventana 1

  sudo tcpdump -i any -n -Ss 0 -Xx host [Ip]

- Ventana 2

  perl -e 'print "M-SEARCH * HTTP/1.1\r\nHost:239.255.255.250:1900\r\nST:upnp:rootdevice\r\nMan:\"ssdp :discover\"\r\nMX:3\r\n\r\n"' > /dev/udp/[Ip]/1900

Si SSDP está expuesto a internet en la ventana 1, se recibirá información del dispositivo al cual se realizó la consulta SSDP.

INFORMACIÓN DE LOS CAMPOS DEL REPORTE:

Campo	Descripción
Vulnerabilidad	Nombre de la vulnerabilidad reportada
Dirección IP	Dirección IP del host
Puerto	Puerto desde donde se obtiene la respuesta SSDP
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
status_EcuCERT	Online: vulnerabilidad reportada por *Feeds* y comprobada por el EcuCERT en el timestamp_EcuCERT Offline: Vulnerabilidad reportada por *Feeds*, pero en el timestamp_EcuCERT no se detectó.
as_name	Nombre del ASN al que pertenece la dirección IP
timestamp	Fecha y hora de comprobación en UTC+0
ip	Dirección IP del host
protocol	Protocolo por el que ingresó la respuesta (UDP)
port	Puerto desde donde se obtiene la respuesta SSDP
hostname	DNS reverso del host
tag	Siempre será SSDP
header	La cabecera HTTPU (HTTP sobre UDP) que fue recibida
asn	ASN de la red donde se encuentra el host
geo	País donde se encuentra el host
region	Estado / Provincia / Región donde se encuentra el host
city	Ciudad donde se encuentra el host
systime	Tiempo GMT cuando la respuesta fue creada
cache_control	cache-control - Cuanto espero para la comunicación
location	URL donde el servicio XML está localizado
server	Información del host que soporta UDAP
search_target	Valor objetivo buscado (ST)
unique_service_name	Campo USN que contiene compilación de uuid:uuid_ del host::ST_de respuesta

4. ACCIONES RECOMENDADAS

Verificación de la IP de origen

Rechazar cualquier tráfico UDP con direcciones falsificadas (spoofed). El IETF publicó como un ISP puede filtrar el tráfico de red para rechazar los paquetes con direcciones de origen no accesibles, que hacen que el dispositivo de enrutamiento

evalúe si es posible llegar a la dirección IP de origen del paquete a través de la interfaz que transmitió el paquete, si no es posible es probable que el paquete tenga una dirección IP de origen falso.

Catalogación de tráfico (Traffic Shaping)

Limitar respuestas a las peticiones UDP. Requiere de pruebas para descubrir el límite óptimo que no interfiera con el tráfico legítimo. La IETF describe algunos métodos en las RFCs 2475 y 3260 para controlar el tráfico, actualmente muchos dispositivos de red ofrecen estas funciones en su software.

Bloqueo de puerto

De no ser utilizado el puerto 1900 UDP, limitar su accesibilidad desde Internet y que sea accesible únicamente desde la red interna.

5. REFERENCIAS

- https://chargenscan.shadowserver.org/
- http://tools.ietf.org/html/bcp38
  (Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing)
- http://tools.ietf.org/html/bcp84
  (Ingress Filtering for Multihomed Networks)
- https://www.us-cert.gov/ncas/alerts/TA14-017A
- http://openssdpproject.org/