Open mDNS

(mDNS: multicast Domain Name System)

1. INTRODUCCIÓN

El propósito de mDNS es resolver nombres de host en direcciones IP dentro de pequeñas redes que no incluyan un servidor local de nombres. Se utiliza en redes locales para descubrir dispositivos y servicios como por ejemplo: impresoras, teléfonos o sistemas de almacenamiento conectado a red (NAS). Los "daemons"[1] mDNS están disponibles para sistemas operativos Windows, OS X y Linux, y utiliza esencialmente las mismas interfaces de programación, formatos de paquetes y operación como el unicast sistema de nombres de dominio (DNS). mDNS está diseñado para trabajar de manera independiente o puede trabajar con servidores DNS Unicast.

2. RIESGO

mDNS es un problema muy común en servidores Linux que mantienen el servicio de avahi-daemon (mDNS) expuesto a internet corriendo en el puerto 5353/UDP.

Este servicio al ser mal utilizado, puede generar ataques de denegación de servicio por inundación de paquetes, ya que permite la amplificación de peticiones a terceros consumiendo así nuestro ancho de banda, de la misma manera un atacante puede extraer información del servicio mDNS enviando paquetes UDP especialmente diseñados.

Normalmente este servicio está abierto sin ningún tipo de uso, porque se instaló un servidor por defecto y quedó abierto sin ninguna protección.

3. DETECCIÓN

Para verificar esta vulnerabilidad se puede ejecutar el siguiente comando:

nmap IP -sU -p 5353

Donde:

[1] **Daemons (Disk And Execution MONitor):** es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario

Argumento	Explicación
nmap:	Comando para ejecución de Netcat
IP	La dirección IP del sistema a verificar
-sU	Determina UDP
-p	Selecciona el puerto
5353	Puerto No. 5353 por el cual se enviara la respuesta del servicio

Ejemplo:

nmap 181.199.xxx.xxxx -sU -p 5353

El resultado de la ejecución de este comando es:

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2017-01-05 10:10 ECT
Nmap scan report for mail.xxxxxxx.xx (181.199.xxx.xxx)
Host is up (0.0031s latency).
PORT     STATE SERVICE
5353/udp open  zeroconf

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

Lo cual indica que la dirección 181.199.xxx.xxxx tiene habilitado el servicio mDNS y que el mismo puede ser usado sin restricciones.

INFORMACIÓN DE LOS CAMPOS DEL REPORTE

Campo	Descripción
vulnerabilidad	Hace referencia al nombre de la vulnerabilidad
direccion_ip	Dirección IP del dispositivo en cuestión
puerto	Puerto que responde a la vulnerabilidad
timestamp_EcuCERT	Tiempo en que la IP fue probada por el ECUCERT GMT-5
as_name	Nombre del ASN
status_EcuCERT	**Estado de la vulnerabilidad** **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.
timestamp	Fecha y Hora en que el sistema correspondiente a la dirección IP UTC +0 fue evaluada respecto a la vulnerabilidad
ip	La dirección IP del sistema evaluado
protocol	Protocolo en el cual vino la respuesta del sistema
port	Puerto por el cual vino la respuesta del Chargen
hostname	Resolución reversa del sistema evaluado
tag	mdns
asn	La ASN correspondiente a la dirección IP
geo	País en el que se encuentra el sistema

Campo	Descripción
region	Provincia en la que se encuentra el sistema
city	Ciudad en la que se encuentra el sistema
naics	Código de Sistema de Clasificación Industrial de América del Norte
sic	Código Estándar de Clasificación Industrial
mdns_name	El nombre trivial .local que a veces se devuelve en respuesta a la detección inicial de _services._dns-sd._udp.local. Este campo está a menudo vacío.
mdns_ipv4	La (s) dirección (es) IPv4 que a veces se devuelven en respuesta a la sonda inicial. Este campo está a menudo vacío.
mdns_ipv6	La (s) dirección (es) IPv6 que a veces se devuelven en respuesta a la sonda inicial. Este campo está a menudo vacío.
services	Los servicios que el host está ejecutando en respuesta a la consulta de la lista de información con "_services._dns-sd._udp.local"
workstation_name	El nombre mdns que se devuelve en respuesta a la consulta mDNS de seguimiento para "_workstation._tcp.local"
workstation_ipv4	Las direcciones IPv4 que se devuelven en respuesta a la consulta mDNS de seguimiento para "_workstation._tcp.local"
workstation_ipv6	Las direcciones IPv6 que se devuelven en respuesta a la consulta mDNS de seguimiento para "_workstation._tcp.local"
workstation_info	Información sobre el host que respondió a la consulta de "_workstation._tcp.local". Puede contener nombres, direcciones MAC, etc.
http_name	El nombre mdns que se devuelve en respuesta a la consulta mDNS de seguimiento para "_http._tcp.local".
http_ipv4	Las direcciones IPv4 que se devuelven en respuesta a la consulta de mDNS de seguimiento para "_http.ttcp.local"
http_ipv6	Las direcciones IPv6 que se devuelven en respuesta a la consulta mDNS de seguimiento para "_http.ttp.local"
http_ptr	Contiene información que parece un nombre trivial y cadenas _local de mdns.
http_info	Más información sobre el dispositivo http es respuesta a la consulta de "_http._tcp.local".
http_target	Nombre del servidor HTTP. Por lo general, sólo el contenido del campo http_name con un ".0"
http_port	El puerto en el que parece estar escuchando el servidor http.

4. ACCIONES RECOMENDADAS

- Detener el servicio

  - ✓ Sobre Linux ejecutar el comando
    - “service avahi-daemon stop”
    - “chkconfig avahi-daemon off”

  - ✓ En versiones más actuales ejecutar
    - “systemctl stop avahi-daemon”
    - “systemctl disable avahi-daemon”

- Configurar el firewall para bloquear el tráfico de paquetes TCP y UDP hacia el puerto 5353.

5. REFERENCIAS

- http://eloy-mp.com/wordpress262/avahi-zeroconf-en-linux/
- https://csirt.cedia.org.ec/how-to/instalacion/ataques-de-amplificacion-basados-en-udp/mdns/
- http://www.securityweek.com/mdns-can-be-used-amplify-ddos-attacks-researcher
- http://www-01.ibm.com/support/docview.wss?uid=swg21699497
- https://github.com/chadillac/mdns_recon