# Open Portmapper

## 1. INTRODUCCIÓN

Portmapper (también conocido como rpcbind, portmap o RPC Portmapper) es un servicio de llamadas a procedimientos remotos de Open Network Computing (ONC RPC) que se ejecuta en nodos de red que proporcionan otros servicios de ONC RPC.

Cuando un cliente está buscando el servicio adecuado, Portmapper es consultado para ayudar con la búsqueda, cuando se realiza la consulta, el tamaño de la respuesta varía dependiendo de qué servicios RPC están operando en el host.

## 2. RIESGO

Se puede abusar del protocolo de Portmapper basado en UDP para amplificar el tráfico en ataques de denegación de servicio. Los servidores que ejecuten Portmapper son vulnerables a ataques de denegación de servicio reflexivos distribuidos (DRDoS).

El atacante genera una gran cantidad de paquetes UDP con direcciones IP de origen suplantadas para que parezca que los paquetes provienen del destino adecuado. Estos paquetes UDP se envían a los servidores de Portmapper (puerto 111)

Portmapper puede funcionar tanto con puerto TCP o UDP 111, UDP se utiliza para que una solicitud de este tipo reciba una respuesta amplificada.

Los ataques de reflexión DDoS afecta gravemente a las empresas y usuarios. Portmapper es un método para este tipo de ataque, los cuales se centraron principalmente en sitos de juegos, hosting e infraestructura de Internet. Este servicio tiene el potencial para ser utilizado en ataques de amplificación para llevar a cabo ataques de denegación de servicios; además puede ser utilizado para obtener una gran cantidad de información sobre el objetivo, incluyendo el NFS de ese dispositivo.

Portmapper representa un vector para la amplificación de los ataques DDoS a través de Internet. Los administradores y organizaciones deben revisar su uso como un servicio de Internet disponible en su entorno, utilizado para ataques DDoS reflexión o amplificación. De pruebas realizadas por Level3 se obtuvo los siguientes resultados peticiones de 68 bytes tuvieron una respuesta amplificada de 486 bytes, 1930 bytes y cuantificaron el tamaño promedio de un ataque de amplificación en un factor de amplificación de 18.3x.

## 3. DETECCIÓN

El comando shell para imitar una exploración portmapper es:

rpcinfo -T udp -p [IP]

Si el puerto está abierto se obtiene una respuesta similar a la presentada en la siguiente figura:

```
$ rpcinfo -T udp -p AAA.BBB.CCC.DDD
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   udp  32768  nlockmgr
    100021    3   udp  32768  nlockmgr
    100021    4   udp  32768  nlockmgr
    100021    1   tcp  34848  nlockmgr
    100021    3   tcp  34848  nlockmgr
    100021    4   tcp  34848  nlockmgr
    100005    1   udp    751  mountd
    100005    1   tcp    754  mountd
    100005    2   udp    751  mountd
    100005    2   tcp    754  mountd
    100005    3   udp    751  mountd
    100005    3   tcp    754  mountd
    100024    1   udp  32770  status
    100024    1   tcp  47090  status
```

**Fuente:** http://blog.level3.com/security/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry/

## INFORMACIÓN DE LOS CAMPOS DEL REPORTE:

| Campo | Descripción |
|---|---|
| Vulnerabilidad | Hace referencia al nombre de la vulnerabilidad |
| Dirección IP | Dirección IP del dispositivo en cuestión |
| Puerto | Puerto que responde a la vulnerabilidad |
| timestamp_EcuCERT | Fecha y hora de comprobación de EcuCERT en GMT -5 |
| as_name | Nombre del ASN al que pertenece la dirección IP |
| status_EcuCERT | Online: vulnerabilidad reportada por *Stakeholders* y comprobada por el EcuCERT en el timestamp_EcuCERT<br>Offline: Vulnerabilidad reportada por *Stakeholders*, pero en el timestamp_EcuCERT no se detectó. |
| 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 Chargen |
| hostname | DNS reverso del host |
| tag | Siempre será chargen |
| 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 |
| naics | Código del Sistema de Clasificación Industrial de América del Norte |

| Campo | Descripción |
|---|---|
| sic | Código del Sistema de Clasificación Industrial Estándar |
| programs | Lista de programas separados por (;) al cual portmapper tiene acceso. El formato de cada entrada es "[número del programa] [versión del programa] [puerto/protocolo];" |
| mountd_port | Puerto mountd que se probó para las exportaciones NFS (si se encuentra mountd que se ejecuta en el host) |
| exports | Lista de exportaciones NFS, separadas por (;), que el host tiene disponible. El formato es: "[directorio exportado] [lista del grupo de restricciones de la exportación (si existen)];" |

## 4. ACCIONES RECOMENDADAS

- Desactivar Portmapper junto con NFS, NIS y todos los demás servicios de RPC a que estén abiertos. En situaciones en las que los servicios deben permanecer activos, se debe configurar qué direcciones IP pueden llegar a dichos servicios y, posteriormente, cambio a TCP-only para evitar ser parte de ataques DDoS en el futuro. Es posible que esta solución influya en el servicio NFS (a menos que usted esté utilizando NFSv4 el cual no interactúa con portmapper).

- Configurar el firewall para que limite las solicitudes entrantes del servicio de Portmapper según una lista específica de clientes o redes, o para que las bloquee en su totalidad.

## 5. REFERENCIAS


- https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-Portmapper
- http://blog.level3.com/security/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry/
- https://www.us-cert.gov/ncas/alerts/TA14-017A
- https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-Portmapper
- https://kb.iweb.com/hc/es/articles/230267968-Gu%C3%ADa-para-evitar-las-problemas-de-amplificaci%C3%B3n-del-servicio-Portmapper
- https://tools.ietf.org/html/rfc1833
- https://www.centos.org/docs/5/html/Deployment_Guide-en-US/ch-nfs.html