Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Vulnerable service

There are a number of different vulnerable service reports that we send out, these vary from services that can be exploited to be used within a Distributed Denial of Service (DDOS) attack to services that are exposed to leak information or allow them to be controlled. Some of these services can simply be firewalled off from the internet at your border without causing any issues, however, some require further configuration. Please see below for further information on these reports and configuration options.

UDP DDoS Reflectors

UDP DDoS reflectors are insecurely configured services which are abused in order to carry out Distributed Denial of Service attacks. In these attacks, an attacker will spoof a victim IP address to send a series of requests to a host running an open UDP reflector service. The host's response, often much larger than the initial request, will then be reflected/directed to the victim host causing a denial of service attack.

Open DNS Resolvers

An Open DNS resolver is a DNS server that will answer recursive queries from any host on the internet.

For information on securing your DNS service, please see:

https://www.us-cert.gov/ncas/alerts/TA13-088A [1]

https://www.shadowserver.org/wiki/pmwiki.php/Services/DNS-open-resolvers [2]

NTP Mode 6/7

NTP servers are frequently used in denial of service attacks through the use of control queries. Any NTP server that responds to either a monlist or READVAR query can be abused in order to carry out these attacks. To test your host, run the following commands from an external *nix-based host with the NTP service installed:

For mode 6 or READVAR:

```
ntp -c rv <IP>
```

For mode 7 or monlist:

```
ntpdc -c monlist <IP>
```

For information on securing your NTP service, please see:

https://www.team-cymru.org/secure-ntp-template.html [3]

https://www.shadowserver.org/wiki/pmwiki.php/Services/NTP-Version [4]

SNMP

The Simple Network Management Protocol is used on a variety of devices to retrieve information about or change various settings on a device. Each device is configured with a “community” string that needs to be supplied in each request sent sent to the device by an SNMP client. For SNMP devices not running SNMPv3, no further authentication information other than the community string is required in order to gather information from the device.

The string “public” is used as the default community string for many devices and can be used to retrieve/gather information about the device such as it's hostname, interfaces configured and much more. By leaving this default string in place and by leaving the device open to the internet, the device also be used to generate large responses in order to carry out denial of service attacks.

An SNMP device can be secured through the following methods:

- Enable SNMPv3 and SNMP authentication
- Change the community string to something other than “public”
- Configure access controls on the device allowing access only from selected hosts, such as a management station
- Deny access inbound on your border device, with permit statements for select devices

To test your host, run the following commands from an external *nix-based host with the snmpwalk installed:

```
snmpwalk -v 2c -c public <IP> 1.3.6.1.2.1.1.1
```

For more information, please see:

https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-SNMP [5]

Chargen

The Character Generator Protocol (CHARGEN) is a service of the Internet Protocol Suite defined in RFC 864 in 1983 by Jon Postel. It is intended for testing, debugging, and measurement purposes. The protocol is rarely used, as its design flaws allow ready misuse. In this case it's best to disable the service or firewall it from the internet.

To test your host, run the following commands from an external *nix-based host with the netcat installed:

```
nc -u <IP> 19
```

and type in a few bits of text, followed by a carriage return. If chargen is enabled, expect to see a fair amount of random text to appear on your screen.

https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-Chargen [6]

Information Leak

NAT-PMP

NAT-PMP allows internal, trusted users to request port forwarding rules on NAT devices allowing external hosts to access internal resources. Examples of usage could be Back-to-my-mac, file sharing functionality, game server hosting. Once a NAT-PMP enabled device receives a NAT-PMP message, it will manipulate it's routing and/or firewall rules in order to fulfill the request.

If NAT-PMP is enabled on an external, untrusted interface, the device can be exploited in the following ways:

- Interception of internal NAT traffic
- Interception of external traffic
- Unwanted access to NAT client resources
- Denial of service against host services
- Information disclosure about the NAT-PMP device

For more information on this vulnerability, please see:

https://community.rapid7.com/community/metasploit/blog/2014/10/21/r7-2014-17-nat-pmp-implementation-and-configuration-vulnerabilities [7]

https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-NATPMP [8]

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/vulnerable-service

Links
[1] https://www.us-cert.gov/ncas/alerts/TA13-088A
[2] https://www.shadowserver.org/wiki/pmwiki.php/Services/DNS-open-resolvers
[3] https://www.team-cymru.org/secure-ntp-template.html
[4] https://www.shadowserver.org/wiki/pmwiki.php/Services/NTP-Version
[5] https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-SNMP
[6] https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-Chargen
[7] https://community.rapid7.com/community/metasploit/blog/2014/10/21/r7-2014-17-nat-pmp-implementation-and-configuration-vulnerabilities
[8] https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-NATPMP