

Defining Strategies to Protect Against UDP Diagnostic Port Denial-of-Service Attacks

Document ID: 13367

Introduction

Prerequisites

Requirements

Components Used

Conventions

Problem Description

The UDP Diagnostic Port Attack

Defend Against Attacks Directly to Network Devices

Disable UDP Diagnostic Ports

Prevent the Network From Unwittingly Hosting an Attack

Prevent Transmission of Invalid IP Addresses

Prevent Reception of Invalid IP Addresses

Appendix: Description of Small Servers

Related Information

Introduction

There is a potential denial-of-service attack at ISPs that targets network devices.

- **User Datagram Protocol (UDP) diagnostic port attack:** A sender transmits a volume of requests for UDP diagnostic services on the router. This causes all CPU resources to be consumed to service the phony requests.

This document describes how the potential UDP diagnostic port attack occurs and suggests the methods to use with Cisco IOS® software in order to defend against it.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions. Some of the commands referred to in this document are only available starting in Cisco IOS Software Releases 10.2(9), 10.3(7), and 11.0(2), and all subsequent releases. These commands are the default in Cisco IOS Software Release 12.0 and later.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Problem Description

The UDP Diagnostic Port Attack

By default, the Cisco router has a series of diagnostic ports enabled for certain UDP and TCP services. These services include echo, chargen, and discard. When a host attaches to these ports, a small amount of CPU capacity is consumed to service these requests.

If a single attacking device sends a large barrage of requests with different, random, phony source IP addresses, it is possible that the Cisco router becomes overwhelmed and slows down or fails.

The external manifestation of the problem includes a process table full error message (%SYS-3 NOPROC) or a very high CPU utilization. The exec command **show process** shows a lot of processes with the same name, such as "UDP Echo."

Defend Against Attacks Directly to Network Devices

Disable UDP Diagnostic Ports

Any network device that has UDP and TCP diagnostic services needs to be protected by a firewall or have the services disabled. For a Cisco router, this can be accomplished by using these global configuration commands.

```
no service udp-small-servers
no service tcp-small-servers
```

See the Appendix for further information on these commands. The commands are available starting in Cisco IOS Software Releases 10.2(9), 10.3(7), and 11.0(2) and all subsequent releases. These commands are the default in Cisco IOS Software Release 12.0 and later.

Prevent the Network From Unwittingly Hosting an Attack

Since a primary mechanism of denial-of-service attacks is the generation of traffic sourced from random IP addresses, Cisco recommends filtering traffic destined for the Internet. The basic concept is to throw away packets with invalid source IP addresses as they enter the Internet. This does not prevent the denial-of-service attack on your network. However, it helps the attacked parties rule out your location as the source of the attacker. In addition, it prevents the use of your network for this class of attacks.

Prevent Transmission of Invalid IP Addresses

By filtering packets on your routers that connect your network to the Internet, you can permit only packets with valid source IP addresses to leave your network and get into the Internet.

For example, if your network consists of network 172.16.0.0, and your router connects to your ISP using a FDDI0/1 interface, you can apply the access list like this:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log 1

interface Fddi 0/1
ip access-group 111 out
```

¹ The last line of the access list determines if there is any traffic with an invalid source address that enters the Internet. This helps to locate the source of the possible attacks.

Prevent Reception of Invalid IP Addresses

For ISPs who provide service to end networks, Cisco highly recommends the validation of incoming packets from your clients. This can be accomplished by the use of inbound packet filters on your border routers.

For example, if your clients have these network numbers connected to your router through an FDDI interface named "FDDI 1/0", you can create this access list.

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0
```

```
access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log
```

```
interface Fddi 1/0
ip access-group 111 in
```

Note: The last line of the access list determines if there is any traffic with an invalid source address that enters the Internet. This helps to locate the source of the possible attack.

Appendix: Description of Small Servers

The small servers are servers (daemons, in UNIX parlance) that run in the router which are useful for diagnostics. Therefore, they are on by default.

The commands for the TCP and UDP small servers are:

- **service tcp-small-servers**
- **service udp-small-servers**

If you do not want your router to provide any non-routing services, turn them off (using the **no** form of the previous commands).

The TCP small servers are:

- **Echo** Echoes back whatever you type. Type the command **telnet x.x.x.x echo** to see.
- **Chargen** Generates a stream of ASCII data. Type the command **telnet x.x.x.x chargen** to see.
- **Discard** Throws away whatever you type. Type the command **telnet x.x.x.x discard** to see.
- **Daytime** Returns system date and time, if correct. It is correct if you run NTP or have set the date and time manually from the exec level. Type the command **telnet x.x.x.x daytime** to see.

The UDP small servers are:

- **Echo** Echoes the payload of the datagram you send.
- **Discard** Silently pitches the datagram you send.
- **Chargen** Pitches the datagram you send and responds with a 72 character string of ASCII characters terminated with a CR+LF.

Note: Almost all UNIX boxes support the small servers previously listed. The router also offers finger service and async line bootp service. These can be independently turned off with the configuration global commands **no service finger** and **no ip bootp server**, respectively.

Related Information

- [Cisco IOS Software](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Dec 27, 2007

Document ID: 13367
