防止UDP診斷埠拒絕服務攻擊

目錄

簡介

ISP存在以網路裝置為目標的潛在拒絕服務攻擊。

- **使用者資料包協定(UDP)診斷埠攻擊**：傳送方在路由器上傳輸大量的UDP診斷服務請求。這會導致所有CPU資源被消耗為處理虛假請求。

本檔案將說明如何發生潛在的UDP診斷連線埠攻擊，並提供與Cisco IOS®軟體搭配使用的方法以抵禦攻擊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。本文檔中提及的一些命令僅在Cisco IOS軟體版本10.2(9)、10.3(7)和11.0(2)以及所有後續版本中可用。這些命令是Cisco IOS軟體版本12.0及更高版本的預設命令。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

問題描述

UDP診斷埠攻擊

預設情況下，思科路由器為某些UDP和TCP服務啟用了一系列診斷埠。這些服務包括echo、chargen和discard。當主機連線到這些埠時，會消耗少量CPU容量來滿足這些請求。

如果單個攻擊裝置傳送大量具有不同隨機假源IP地址的請求，則思科路由器可能會不堪重負，速度減慢或發生故障。

問題的外部表現形式包括進程表完全錯誤消息(%SYS-3 NOPROC)或CPU使用率非常高。exec命令**show process**顯示許多同名進程，例如「UDP Echo」。

防禦直接針對網路裝置的攻擊

禁用UDP診斷埠

任何具有UDP和TCP診斷服務的網路裝置都需要受到防火牆的保護或禁用這些服務。對於Cisco路由器，可以使用這些全域性配置命令來完成此操作。

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

如需這些命令的詳細資訊，請參閱附錄。可從Cisco IOS軟體版本10.2(9)、10.3(7)和11.0(2)及所有後續版本開始使用這些命令。這些命令是Cisco IOS軟體版本12.0及更高版本的預設命令。

防止網路在不知不覺中發動攻擊

由於拒絕服務攻擊的主要機制是產生源自隨機IP地址的流量，思科建議過濾目的地為網際網路的流量。基本概念是在資料包進入Internet時丟棄其源IP地址無效的資料包。這無法防止對網路的拒絕服務攻擊。但是，它可以幫助受攻擊方排除您作為攻擊源的位置。此外，它還可以防止將您的網路用於此類攻擊。

阻止傳輸無效IP地址

通過在將您的網路連線到Internet的路由器上過濾資料包，您可以僅允許具有有效源IP地址的資料包離開您的網路並進入Internet。

例如，如果您的網路由網路172.16.0.0組成，並且您的路由器使用FDDI0/1介面連線到ISP，則可以應用訪問清單，如下所示：

```
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]存取清單的最後一行可判斷是否有任何流量具有進入網際網路的無效來源位址。這有助於找到可能攻擊的來源。

阻止接收無效IP地址

對於向終端網路提供服務的ISP，思科強烈建議驗證來自您客戶端的傳入資料包。這可以通過在邊界路由器上使用入站資料包過濾器來實現。

例如，如果您的使用者端透過名為「FDDI 1/0」的FDDI介面將這些網路編號連線到您的路由器，則您可以建立此存取清單。

```
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
```
注意：訪問清單的最後一行確定是否有任何包含無效源地址的流量進入Internet。這有助於確定可能攻擊的來源。

附錄：小型伺服器說明

小型伺服器是在路由器中運行的伺服器（UNIX術語中的守護程式），對診斷非常有用。因此，預設情況下它們處於開啟狀態。

TCP和UDP小型伺服器的命令如下：

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

如果不希望路由器提供任何非路由服務，請將其關閉(使用前面命令的**no**形式)。

TCP小型伺服器包括：

- **Echo** — 回顯您鍵入的任何內容。鍵入命令**telnet x.x.x.x echo**以進行檢視。
- **Chargen** — 生成ASCII資料流。鍵入命令**telnet x.x.x.x chargen**檢視。
- **丟棄** — 丟棄鍵入的任何內容。鍵入命令**telnet x.x.x.x discard**進行檢視。
- **Daytime** — 返回系統日期和時間（如果正確）。如果您運行NTP或者已經從exec級別手動設定日期和時間，則是正確的。鍵入命令**telnet x.x.x.x daytime**以檢視。

UDP小型伺服器包括：

- **Echo** — 回顯您傳送的資料包的負載。
- **Discard** — 以靜默方式投遞您傳送的資料包。
- **Chargen** — 對傳送的資料包進行分隔，並用以CR+LF結尾的72個字元的ASCII字元進行響應。

注意：**幾**乎所有UNIX盒都支援之前列出的小型伺服器。路由器還提供手指服務和非同步線路bootp服務。分別使用**no service finger**和**no ip bootp server** 配置全域性命令可以單獨關閉這些功能。

相關資訊

- Cisco IOS軟體
- 技術支援 - Cisco Systems