Definition von Strategien zum Schutz vor Denial-of-Service-Angriffen durch UDP-Diagnoseports

Inhalt

Einführung

Es besteht ein potenzieller Denial-of-Service-Angriff auf ISPs, der auf Netzwerkgeräte abzielt.

- **User Datagram Protocol (UDP)-Diagnoseport-Angriff:** Ein Sender überträgt ein Volumen von Anfragen für UDP-Diagnoseservices auf den Router. Dies führt dazu, dass alle CPU-Ressourcen für die Bearbeitung der angefochtenen Anfragen verwendet werden.

In diesem Dokument wird beschrieben, wie der potenzielle UDP-Diagnose-Port-Angriff auftritt, und es werden Methoden vorgeschlagen, die mit der Cisco IOS®-Software zum Schutz vor diesem Angriff verwendet werden.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt. Einige der in diesem Dokument erwähnten Befehle sind nur ab den Cisco IOS Software-Versionen

10.2(9), 10.3(7) und 11.0(2) sowie allen nachfolgenden Versionen verfügbar. Diese Befehle sind die Standardbefehle der Cisco IOS Software, Version 12.0 und höher.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Problembeschreibung

Der UDP-Diagnoseport-Angriff

Standardmäßig sind auf dem Cisco Router eine Reihe von Diagnose-Ports für bestimmte UDP- und TCP-Services aktiviert. Zu diesen Services gehören Echo, Chargen und Disard. Wenn ein Host an diese Ports angeschlossen wird, wird eine geringe CPU-Kapazität für diese Anforderungen belegt.

Wenn ein einziges Angriffsgerät eine große Anzahl von Anfragen mit unterschiedlichen, zufälligen und gefälschten Quell-IP-Adressen sendet, ist es möglich, dass der Cisco Router überlastet wird, langsamer wird oder ausfällt.

Die externe Manifestation des Problems beinhaltet eine vollständige Fehlermeldung in der Prozesstabelle (`%SYS-3 NOPROC`) oder eine sehr hohe CPU-Auslastung. Der exec-Befehls-**Anzeigeprozess** zeigt eine Vielzahl von Prozessen mit demselben Namen an, z. B. "UDP Echo".

Schutz vor Angriffen direkt auf Netzwerkgeräte

Deaktivieren von UDP-Diagnoseports

Jedes Netzwerkgerät mit UDP- und TCP-Diagnoseservices muss durch eine Firewall geschützt werden oder die Services deaktiviert werden. Bei einem Cisco Router kann dies mithilfe der folgenden globalen Konfigurationsbefehle erfolgen.

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

Weitere Informationen zu diesen Befehlen finden Sie im Anhang. Die Befehle sind ab den Cisco IOS Software-Versionen 10.2(9), 10.3(7) und 11.0(2) sowie allen nachfolgenden Versionen verfügbar. Diese Befehle sind die Standardbefehle der Cisco IOS Software, Version 12.0 und höher.

Verhindern, dass das Netzwerk unbeabsichtigt einen Angriff hostet

Da ein primärer Mechanismus für Denial-of-Service-Angriffe die Generierung von Datenverkehr ist, der von zufälligen IP-Adressen stammt, empfiehlt Cisco, den für das Internet bestimmten Datenverkehr zu filtern. Das Grundkonzept besteht darin, Pakete mit ungültigen Quell-IP-

Adressen wegzuwerfen, wenn diese das Internet betreten. Dies verhindert jedoch nicht den Denial-of-Service-Angriff auf Ihr Netzwerk. Es hilft den Angreifern jedoch, Ihren Standort als Quelle des Angreifers auszuschließen. Darüber hinaus wird die Verwendung des Netzwerks für diese Angriffsklasse verhindert.

Verhindern der Übertragung ungültiger IP-Adressen

Wenn Sie Pakete auf Ihren Routern filtern, die Ihr Netzwerk mit dem Internet verbinden, können Sie nur Paketen mit gültigen Quell-IP-Adressen erlauben, das Netzwerk zu verlassen und in das Internet zu gelangen.

Wenn Ihr Netzwerk beispielsweise aus dem Netzwerk 172.16.0.0 besteht und Ihr Router über eine FDDI0/1-Schnittstelle eine Verbindung zu Ihrem ISP herstellt, können Sie die Zugriffsliste wie folgt anwenden:

```
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]Die letzte Zeile der Zugriffsliste bestimmt, ob ein Datenverkehr mit einer ungültigen Quelladresse im Internet eingeht. Dies hilft, die Quelle möglicher Angriffe zu finden.

Verhindern des Empfangs ungültiger IP-Adressen

Für ISPs, die Dienste für Endnetzwerke bereitstellen, empfiehlt Cisco nachdrücklich die Validierung eingehender Pakete von Ihren Clients. Dies kann durch die Verwendung von eingehenden Paketfiltern auf Ihren Grenzroutern erreicht werden.

Wenn Ihre Clients beispielsweise über eine FDDI-Schnittstelle mit dem Namen "FDDI 1/0" über diese Netzwerknummern mit dem Router verbunden sind, können Sie diese Zugriffsliste erstellen.

```
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
```

Hinweis: Die letzte Zeile der Zugriffsliste bestimmt, ob Datenverkehr mit einer ungültigen Quelladresse im Internet vorhanden ist. Dies hilft, die Quelle des möglichen Angriffs zu finden.

Anhang: Beschreibung der kleinen Server

Bei den kleinen Servern handelt es sich um Server (Daemon, UNIX-Darstellung), die im Router ausgeführt werden und für Diagnosen nützlich sind. Daher sind sie standardmäßig aktiviert.

Die Befehle für kleine TCP- und UDP-Server lauten wie folgt:

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

Wenn Ihr Router keine Nicht-Routing-Services bereitstellen soll, deaktivieren Sie diese Services (mithilfe der **no-**Form der vorherigen Befehle).

Die kleinen TCP-Server sind:

- **Echo** - Wählt zurück, was immer Sie eingeben. Geben Sie den Befehl **telnet x.x.x.x echo ein**, um zu sehen.
- **Chargen**: Generiert einen Stream von ASCII-Daten. Geben Sie den Befehl **telnet x.x.x.x.x ein**, um zu sehen.
- **Verwerfen**: Wirft alle eingegebenen Daten weg. Geben Sie den Befehl **telnet x.x.x.x discard ein**, um zu sehen.
- **Daytime** - Gibt das Systemdatum und die Systemzeit zurück, falls korrekt. Es ist richtig, wenn Sie NTP ausführen oder das Datum und die Uhrzeit manuell von der exec-Ebene aus festgelegt haben. Geben Sie den Befehl **telnet x.x.x.x Tageszeit** ein, um zu sehen.

Die UDP-kleinen Server sind:

- **Echo**: Legt die Nutzlast des gesendeten Datagramms fest.
- **Verwerfen**: Es wird ein leises Bild des Datagramms angezeigt, das Sie versenden.
- **Chargen**: Zeichnet das gesendete Datagramm und antwortet mit einer 72-stelligen Zeichenfolge aus ASCII-Zeichen, die mit CR+LF terminiert wird.

Hinweis: Fast alle UNIX-Boxen unterstützen die zuvor aufgeführten kleinen Server. Der Router bietet außerdem einen Fingerdienst und einen asynchronen Line-Bootp-Service an. Diese können unabhängig mit den globalen Konfigurationsbefehlen **ohne Dienstfinger** und **ohne ip bootp server** deaktiviert werden.

Zugehörige Informationen

- Cisco IOS-Software
- Technischer Support – Cisco Systems