UDP 진단 포트 서비스 거부 공격으로부터 보호

목차

소개

ISP에서 네트워크 디바이스를 대상으로 하는 잠재적인 서비스 거부 공격이 있습니다.

- **UDP(User Datagram Protocol) 진단 포트 공격:** 발신자는 라우터에서 UDP 진단 서비스에 대한 요청 볼륨을 전송합니다. 이렇게 하면 모든 CPU 리소스가 가짜 요청을 처리하는 데 사용됩니다.

이 문서에서는 잠재적인 UDP 진단 포트 공격이 발생하는 방법을 설명하고 이를 방어하기 위해 Cisco IOS® 소프트웨어와 함께 사용할 방법을 제안합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다. 이 문서에서 참조하는 명령 중 일부는 Cisco IOS Software 릴리스 10.2(9), 10.3(7) 및 11.0(2) 및 모든 후속 릴리스에서만 사용할 수 있습니다. 이러한 명령은 Cisco IOS Software Release 12.0 이상에서 기본값입니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

문제 설명

UDP 진단 포트 공격

기본적으로 Cisco 라우터에는 특정 UDP 및 TCP 서비스에 대해 활성화된 일련의 진단 포트가 있습니다. 이러한 서비스에는 echo, chargen 및 discard가 포함됩니다. 호스트가 이러한 포트에 연결되면 이러한 요청을 처리하는 데 소량의 CPU 용량이 사용됩니다.

단일 공격 디바이스에서 서로 다른 랜덤 소스 IP 주소를 사용하여 대량의 요청을 전송하는 경우 Cisco 라우터가 오버헤딩되거나 속도가 느려지거나 실패할 수 있습니다.

문제의 외부 표시에 프로세스 테이블 전체 오류 메시지(%SYS-3 NOPROC) 또는 CPU 사용률이 매우 높습니다. exec 명령 **show process는** 동일한 이름의 많은 프로세스(예: "UDP Echo")를 표시합니다.

네트워크 장치에 직접 대한 공격으로부터 보호

UDP 진단 포트 비활성화

UDP 및 TCP 진단 서비스가 있는 네트워크 장치는 방화벽에 의해 보호되거나 서비스를 비활성화해야 합니다. Cisco 라우터의 경우 이러한 전역 컨피그레이션 명령을 사용하여 이를 수행할 수 있습니다.

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

이러한 명령에 대한 자세한 내용은 부록을 참조하십시오. 이 명령은 Cisco IOS Software 릴리스 10.2(9), 10.3(7) 및 11.0(2) 및 모든 후속 릴리스부터 사용할 수 있습니다. 이러한 명령은 Cisco IOS Software Release 12.0 이상에서 기본값입니다.

네트워크를 무의식적으로 공격을 호스트하는 것을 방지

DoS(denial-of-service) 공격의 기본 메커니즘은 랜덤 IP 주소에서 소싱된 트래픽 생성이므로, Cisco는 인터넷으로 향하는 트래픽을 필터링하는 것을 권장합니다. 기본 개념은 잘못된 소스 IP 주소가 있는 패킷을 인터넷에 입력할 때 버리는 것입니다. 이는 네트워크에 대한 서비스 거부 공격을 방지하지 않습니다. 그러나 공격자가 공격자의 소스로 사용자의 위치를 제외하는 데 도움이 됩니다. 또한 이러한 유형의 공격에 네트워크 사용을 방지합니다.

잘못된 IP 주소의 전송 방지

네트워크를 인터넷에 연결하는 라우터에서 패킷을 필터링하면 유효한 소스 IP 주소가 있는 패킷만 네트워크를 떠나 인터넷에 액세스하도록 허용할 수 있습니다.

예를 들어, 네트워크가 네트워크 172.16.0.0으로 구성되고 라우터가 FDDI0/1 인터페이스를 사용하여 ISP에 연결되는 경우 다음과 같은 액세스 목록을 적용할 수 있습니다.

```
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 액세스 목록의 마지막 줄은 인터넷에 잘못된 소스 주소를 가진 트래픽이 있는지 여부를 결정합니다. 이를 통해 가능한 공격의 소스를 찾을 수 있습니다.

잘못된 IP 주소의 수신 방지

엔드 네트워크에 서비스를 제공하는 ISP의 경우, Cisco는 클라이언트에서 들어오는 패킷의 검증을 적극 권장합니다. 이 작업은 경계 라우터에서 인바운드 패킷 필터를 사용하여 수행할 수 있습니다.

예를 들어, 클라이언트가 "FDDI 1/0"이라는 FDDI 인터페이스를 통해 라우터에 연결된 네트워크 번호를 가지고 있는 경우 이 액세스 목록을 생성할 수 있습니다.

```
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
```

참고: 액세스 목록의 마지막 줄은 인터넷에 들어오는 잘못된 소스 주소를 가진 트래픽이 있는지 여부를 결정합니다. 이를 통해 가능한 공격의 소스를 찾을 수 있습니다.

부록: 소규모 서버에 대한 설명

소규모 서버는 라우터에서 실행되는 서버(UNIX 풀의 데몬)로서 진단에 유용합니다. 따라서 기본적으로 설정되어 있습니다.

TCP 및 UDP 소규모 서버에 대한 명령은 다음과 같습니다.

- **서비스 tcp-small-servers**
- **서비스 udp-small servers**

라우터가 비라우팅 서비스를 제공하지 않도록 하려면 이전 명령의 **no** 형식을 사용하여 서비스를 끕니다.

TCP 소규모 서버는 다음과 같습니다.

- **에코**(Echo) - 입력하는 모든 항목을 다시 에코합니다. 볼 **텔넷 x.x.x echo** 명령을 입력합니다.
- **Chargen** - ASCII 데이터의 스트림을 생성합니다. 볼 **텔넷 x.x.x chargen** 명령을 입력합니다.
- **Discard**(폐기) - 입력한 내용을 모두 삭제합니다. **텔넷 x.x.x.x discard** 명령을 입력하여 확인합니다.
- **Daytime**(낮) - 올바른 경우 시스템 날짜와 시간을 반환합니다. NTP를 실행하거나 EXEC 레벨에서 날짜와 시간을 수동으로 설정한 경우 정확합니다. **텔넷 x.x.x.x 낮**에 표시할 명령을 입력합니다.

UDP 소규모 서버는 다음과 같습니다.

- **Echo**(에코) - 보내는 데이터그램의 페이로드를 에코합니다.
- **Discard**(삭제) - 보내는 데이터그램을 자동으로 조정합니다.
- **Chargen** - 보내는 데이터그램을 피싱하고 CR+LF로 종료된 72자의 ASCII 문자로 응답합니다.

참고: 대부분의 UNIX 상자는 이전에 나열된 소규모 서버를 지원합니다. 또한 이 라우터는 핑거 서비스 및 비동기 회선 부팅 서비스를 제공합니다. **서비스 핑거**가 **없고** ip bootp **서버**가 **없는** 컨피그레이션 전역 명령과 함께 이러한 명령을 독립적으로 해제할 수 있습니다.

관련 정보

- Cisco IOS 소프트웨어
- Technical Support - Cisco Systems