Cisco Media Experience Engine 5600의 루트 어카운트에 대한 기본 자격 증명 사용 식별 및 완화

Cisco Media Experience Engine 5600의 루트 어카운트에 대한 기본 자격 증명 사용 식별 및 완화

자문 ID: cisco-amb-20110601-mxe

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110601-mxe

개정 1.0

2011년 6월 1일 16:00 UTC(GMT) 공개 릴리스의 경우

목차

Cisco의 대응

이 Applied Mitigation Bulletin은 *Cisco Media Experience Engine 5600의 루트 어카운트에 대한 PSIRT* Security Advisory *Default Credentials(PSIRT* 보안 자문 *기본 자격 증명)*와 함께 제공되는 문서로서 관리자가 Cisco 네트워크 디바이스에 구축할 수 있는 식별 및 완화 기술을 제공합니다.

취약성 특성

Cisco MXE(Media Experience Engine) 5600에는 기본 *비밀번호*로 기본적으로 활성화되는 루트 관리자 계정이 포함되어 있습니다. 이 취약성은 인증 없이, 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 임의의 코드 실행이 허용되거나 정보 공개가 허용되어 공격자가 해당 디바이스에 대한 정보를 학습할 수 있습니다. 익스플로잇을 위한 공격 벡터는 TCP 포트 22를 사용하는 SSH 패킷과 TCP 포트 23을 사용하는 텔넷 패킷을 통해 이루어집니다. 참고: 텔넷은 Cisco MXE 5600에서 기본적으로 비활성화되지만 영향을 받는 디바이스에서 수동으로 활성화하는 경우 익스플로잇 벡터로 사용할 수 있습니다.

이 취약성에는 CVE 식별자 CVE-2011-1623이 할당되었습니다.

취약한 소프트웨어, 영향을 받지 않는 소프트웨어, 그리고 고정된 소프트웨어에 대한 정보는 PSIRT Security Advisory에서 확인할 수 있습니다. PSIRT Security Advisory는 다음 링크에서 확인할 수 있

습니다. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110601-mxe

완화 기법 개요

Cisco 디바이스는 이러한 취약성에 대한 몇 가지 대응책을 제공합니다. 관리자는 이러한 보호 방법을 인프라 디바이스 및 네트워크를 이동하는 트래픽에 대한 일반적인 보안 모범 사례로 고려하는 것이 좋습니다. 이 문서에서는 이러한 기술에 대한 개요를 제공합니다.

Cisco IOS Software는 iACL(infrastructure access control list)을 사용하여 효과적인 익스플로잇 방지 수단을 제공할 수 있습니다. 이 보호 메커니즘은 이 취약성을 악용하려는 패킷을 필터링하고 삭제합니다.

Cisco ASA 5500 Series Adaptive Security Appliance와 Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터용 FWSM(Firewall Services Module)에서는 tACL(transit access control list)을 사용하여 효과적인 익스플로잇 방지 기능을 제공할 수도 있습니다.

이 보호 메커니즘은 이 취약성을 악용하려는 패킷을 필터링하고 삭제합니다.

Cisco IOS NetFlow 레코드는 네트워크 기반 익스플로잇 시도에 대한 가시성을 제공할 수 있습니다.

Cisco IOS Software와 Cisco ASA 및 FWSM 방화벽은 **show** 명령 출력에 표시된 syslog 메시지 및 카운터 값을 통해 가시성을 제공할 수 있습니다.

위험 관리

조직은 이 취약성의 잠재적인 영향을 판단하기 위해 표준 위험 평가 및 완화 프로세스를 따르는 것이 좋습니다. 분류(Triage)란 성공 가능성이 가장 높은 프로젝트를 분류하고 노력을 우선 순위를 정하는 것을 말한다. Cisco는 조직이 정보 보안 팀을 위해 위험 기반 분류 기능을 개발하는 데 도움이 될 문서를 제공했습니다. 보안 취약성 알림에 대한 위험 분류 및 위험 분류 및 프로토타이핑은 조직이 반복 가능한 보안 평가 및 대응 프로세스를 개발하는 데 도움이 될 수 있습니다.

디바이스별 완화 및 식별

주의: 모든 완화 기법의 효과는 제품 혼합, 네트워크 토폴로지, 트래픽 동작, 조직 임무 등 특정 고객 상황에 따라 달라집니다. 모든 컨피그레이션 변경과 마찬가지로, 변경 사항을 적용하기 전에 이 컨피그레이션의 영향을 평가합니다.

완화 및 식별에 대한 구체적인 정보를 다음 장치에 사용할 수 있습니다.

- Cisco IOS 라우터 및 스위치
- Cisco IOS NetFlow
- Cisco ASA 및 FWSM 방화벽

Cisco IOS 라우터 및 스위치

완화: 인프라 액세스 제어 목록

인프라 디바이스를 보호하고 직접 인프라 공격의 위험, 영향 및 효과를 최소화하기 위해 관리자는 인프라 장비에 전송된 트래픽의 정책 시행을 수행하기 위해 iACL(infrastructure access control list)을 구축하는 것이 좋습니다. 관리자는 기존 보안 정책 및 컨피그레이션에 따라 인프라 디바이스

로 전송되는 승인된 트래픽만 명시적으로 허용하여 iACL을 구성할 수 있습니다. 인프라 디바이스를 최대한 보호하려면 구축된 iACL을 IP 주소가 구성된 모든 인터페이스의 인그레스 방향으로 적용해야 합니다. iACL 해결 방법은 공격이 신뢰할 수 있는 소스 주소에서 시작되는 경우 이 취약성에 대한 완벽한 보호를 제공할 수 없습니다.

iACL 정책은 영향을 받는 디바이스로 전송되는 TCP 포트 22의 무단 SSH 패킷과 TCP 포트 23의 텔넷 패킷을 거부합니다. 다음 예에서 192.168.60.0/24은 영향을 받는 디바이스에서 사용하는 IP 주소 공간이며, 192.168.100.1의 호스트는 영향을 받는 디바이스에 액세스해야 하는 신뢰할 수 있는 소스로 간주됩니다. 모든 무단 트래픽을 거부하기 전에 라우팅 및 관리 액세스에 필요한 트래픽을 허용하도록 주의해야 합니다. 인프라 주소 공간은 가능한 경우 사용자 및 서비스 세그먼트에 사용되는 주소 공간과 구분되어야 합니다. 이 주소 지정 방법론을 사용하면 iACL의 구축 및 구축에 도움이 됩니다.

iACL에 대한 추가 정보는 코어 보호: Infrastructure Protection Access Control Lists에 있습니다.

```
 ip access-list extended Infrastructure-ACL-Policy
 ! !-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable ports ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 22
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 23 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in identification of
attacks ! deny tcp any 192.168.60.0 0.0.0.255 eq 22 deny tcp any 192.168.60.0
0.0.0.255 eq 23 ! !-- Explicit deny ACE for traffic sent to addresses configured
within !-- the infrastructure address space ! deny ip any 192.168.60.0 0.0.0.255 ! !-
- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-- with
existing security policies and configurations ! !-- Apply iACL to interfaces in the
ingress direction ! interface GigabitEthernet0/0 ip access-group Infrastructure-ACL-
Policy in
```

인터페이스 액세스 목록으로 필터링하면 ICMP 도달 불가 메시지를 필터링된 트래픽의 소스로 다시 전송합니다. 이러한 메시지를 생성하면 디바이스에서 CPU 사용률이 증가하는 원치 않는 영향을 미칠 수 있습니다. Cisco IOS Software에서 ICMP 연결 불가능 생성은 기본적으로 500밀리초마다 하나의 패킷으로 제한됩니다. ICMP 연결 불가 메시지 생성은 인터페이스 컨피그레이션 명령 no ip unreachable을 사용하여 **비활성화할** 수 **있습니다**. ICMP 연결 불가능 속도 제한은 **ip icmp rate-limit unreachable** *interval-in-ms 전역* 구성 명령을 사용하여 기본값에서 변경할 수 있습니다.

식별: 인프라 액세스 제어 목록

관리자가 인터페이스에 iACL을 적용한 후 **show ip access-lists 명령**은 iACL이 적용된 인터페이스에서 필터링된 TCP 포트 22의 SSH 패킷과 TCP 포트 23의 텔넷 패킷의 수를 식별합니다. 관리자는 필터링된 패킷을 조사하여 이 취약성을 악용하려는 시도인지 확인해야 합니다. **show ip access-lists**의 출력 **예는 다음과** 같습니다.

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq ssh
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq telnet
    30 deny tcp any 192.168.60.0 0.0.0.255 eq ssh (23 matches)
    40 deny tcp any 192.168.60.0 0.0.0.255 eq telnet (17 matches)
    50 deny ip any 192.168.60.0 0.0.0.255
router#
```

앞의 예에서 액세스 목록 Infrastructure-ACL-Policy는 ACE(Access Control List Entry) 라인 30에 대해 TCP 포트 22에서 23개의 SSH 패킷을, ACE 라인**40에 대해 TCP** 포트 **23에서** 17개 텔넷 패킷을

삭제했습니다.

ACE 카운터 및 syslog 이벤트를 사용한 인시던트 조사에 대한 자세한 내용은 Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence 백서를 참조하십시오.

관리자는 ACE 카운터 적중과 같은 특정 조건이 충족될 때 Embedded Event Manager를 사용하여 계측을 제공할 수 있습니다. 보안 컨텍스트의 Embedded Event Manager Applied Intelligence 백서에서는 이 기능 사용 방법에 대한 추가 세부 정보를 제공합니다.

Cisco IOS NetFlow

식별: NetFlow 레코드를 사용한 트래픽 흐름 식별

관리자는 Cisco IOS 라우터 및 스위치에서 Cisco IOS NetFlow를 구성하여 취약성을 악용하려는 시도일 수 있는 트래픽 흐름을 식별할 수 있도록 지원할 수 있습니다. 관리자는 플로우를 조사하여 취약성을 악용하려는 시도인지 또는 올바른 트래픽 플로우인지 확인하는 것이 좋습니다.

```
router#show ip cache flow
IP packet size distribution (2409 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .349 .650 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  89 active, 4007 inactive, 318 added
  4544 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW             38      0.0         9    40      0.0       0.0      15.2
TCP-other          108      0.0         6    40      0.0       0.0      15.5
UDP-TFTP            10      0.0         4    28      0.0       0.0      15.7

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
UDP-other           73      0.0         7    28      0.0       0.0      15.5
Total:             229      0.0         7    35      0.0       0.0      15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.74.110  Et0/1         192.168.13.20   06 C8A7 D4BE     5
Et0/0         192.168.23.20   Et0/1         192.168.226.172 11 2123 540A     1
Et0/0         192.168.53.205  Et0/1         192.168.60.88   11 DEB7 0045     5
Et0/0         192.168.0.115   Et0/1         192.168.60.214  06 F73A 0050    11
Et0/0         192.168.0.30    Et0/1         192.168.60.63   06 A64E 0016     3
Et0/0         192.168.211.52  Et0/1         192.168.113.252 11 17AA 8F11    17
Et0/0         192.168.34.222  Et0/1         192.168.58.190  11 9A8F 2AD3     5
Et0/0         192.168.198.3   Et0/1         192.168.60.104  11 4F4D 0045     1
Et0/0         192.168.240.90  Et0/1         192.168.88.197  06 3D88 0017    15
Et0/0         192.168.0.96    Et0/1         192.168.60.126  06 9621 0017     3
Et0/0         192.168.155.22  Et0/1         192.168.80.13   06 1298 EB6A    10
```

```
Et0/0          192.168.0.20     Et0/1          192.168.60.78    06 1541 0050     3
Et0/0          192.168.0.2      Et0/1          192.168.60.195   06 5419 01BB     5
Et0/0          192.168.223.127  Et0/1          192.168.121.153  06 0613 17E5     7
Et0/0          192.168.0.28     Et0/1          192.168.60.101   06 B5C6 0017     2
Et0/0          192.168.92.207   Et0/1          192.168.43.167   11 1FF5 2815    11
Et0/0          192.168.0.28     Et0/1          192.168.60.139   06 24E9 0050     6
Et0/0          192.168.122.182  Et0/1          192.168.68.21    11 71C2 80BB    11
Et0/0          192.168.18.228   Et0/1          192.168.203.86   11 0630 77B4    16
Et0/0          192.168.0.218    Et0/1          192.168.60.248   06 531B 01BB    15
Et0/0          192.168.26.81    Et0/1          192.168.213.193  06 76D9 11B0     3
Et0/0          192.168.225.144  Et0/1          192.168.28.79    11 FF8F 299D    32
Et0/0          192.168.166.100  Et0/1          192.168.60.217   11 0B47 0045    10
Et0/0          192.168.49.15    Et0/1          192.168.139.203  11 D880 6D41     4
Et0/0          192.168.0.120    Et0/1          192.168.60.41    06 D24F 0016     6
Et0/0          192.168.0.109    Et0/1          192.168.60.189   06 B0B0 0016    11
Et0/0          192.168.0.65     Et0/1          192.168.60.136   06 6110 01BB     2
Et0/0          192.168.0.51     Et0/1          192.168.60.43    06 4090 0050    17
Et0/0          192.168.160.238  Et0/1          192.168.38.104   06 F54E DEE1    14
router#
```

앞의 예에서는 TCP 포트 22의 SSH(16진수 값 0016)와 **TCP** 포트**23**의 **텔넷**(16진수 값 **0017)에** 대한 여러 플로우가 있습니다**계를 참조하십시오.**

TCP 포트 22의 SSH 패킷(16진수 값 0016) 및 TCP 포트 23의 텔넷 패킷(16진수 값 0017)에 대한 트래픽 흐름만 보려면 명령 show **ip cache flow | include SrcIf|**_06_.*0016|0017은 다음과 같이 관련 TCP NetFlow 레코드를 표시합니다.

TCP 흐름

```
router#show ip cache flow | include SrcIf|_06_.*0016|0017
SrcIf          SrcIPaddress     DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Et0/0          192.168.0.30     Et0/1          192.168.60.63   06 A64E 0016     3
Et0/0          192.168.0.120    Et0/1          192.168.60.41   06 D24F 0017     6
Et0/0          192.168.0.109    Et0/1          192.168.60.189  06 B0B0 0016    11
router#
```

Cisco ASA 및 FWSM 방화벽

완화: 통과 액세스 제어 목록

인터넷 연결 지점, 파트너 및 공급업체 연결 지점 또는 VPN 연결 지점이 포함될 수 있는 인그레스 액세스 지점에서 네트워크로 들어오는 트래픽으로부터 네트워크를 보호하려면 관리자가 tACL을 구축하여 정책 적용을 수행하는 것이 좋습니다. 관리자는 승인 받은 트래픽만 인그레스 액세스 포인트에서 네트워크에 들어가도록 명시적으로 허용하거나 기존 보안 정책 및 컨피그레이션에 따라 인증 받은 트래픽이 네트워크를 통과하도록 허용하여 tACL을 구성할 수 있습니다. tACL 해결 방법은 공격이 신뢰할 수 있는 소스 주소에서 시작되는 경우 이 취약성에 대한 완벽한 보호를 제공할 수 없습니다.

tACL 정책은 영향을 받는 디바이스로 전송되는 TCP 포트 22의 무단 SSH 패킷과 TCP 포트 23의 텔넷 패킷을 거부합니다. 다음 예에서 192.168.60.0/24은 영향을 받는 디바이스에서 사용하는 IP 주소 공간이며, 192.168.100.1의 호스트는 영향을 받는 디바이스에 액세스해야 하는 신뢰할 수 있는 소스로 간주됩니다. 모든 무단 트래픽을 거부하기 전에 라우팅 및 관리 액세스에 필요한 트래픽을 허용하도록 주의해야 합니다.

tACL에 대한 추가 정보가 트랜짓 액세스 제어 목록: 에지에서 필터링에 있습니다.

```
! !-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable ports ! access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 22 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 23 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in identification of
attacks ! access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq
22 access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 23 !
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-- with
existing security policies and configurations ! !-- Explicit deny for all other IP
traffic ! access-list tACL-Policy extended deny ip any any ! !-- Apply tACL to
interface(s) in the ingress direction ! access-group tACL-Policy in interface outside
```

식별: 통과 액세스 제어 목록

인터페이스에 tACL이 적용된 후 관리자는 **show access-list 명령**을 사용하여 필터링된 TCP 포트 22의 SSH 패킷 및 TCP 포트 23의 텔넷 패킷 수를 식별할 수 있습니다. 관리자는 필터링된 패킷을 조사하여 이 취약성을 악용하려는 시도인지 확인하는 것이 좋습니다. show access-**list tACL-Policy**의 **출력 예는 다음과** 같습니다.

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 5 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
  192.168.60.0 255.255.255.0 eq ssh (hitcnt=485)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
  192.168.60.0 255.255.255.0 eq telnet (hitcnt=29)
access-list tACL-Policy line 3 extended deny tcp any
  192.168.60.0 255.255.255.0 eq ssh (hitcnt=58)
access-list tACL-Policy line 4 extended deny tcp any
  192.168.60.0 255.255.255.0 eq telnet (hitcnt=16)
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=8)
firewall#
```

앞의 예에서 액세스 목록 tACL-Policy는 신뢰할 수 없는 호스트나 네트워크에서 수신한 TCP 포트 **22**의 **58개 SSH** 패킷 및 TCP 포트 23**의 텔넷** 패킷 **16개를 삭제했습니다.** 또한 syslog 메시지 *106023은* 소스 및 목적지 IP 주소, 소스 및 목적지 포트 번호, 거부된 패킷에 대한 IP 프로토콜을 포함하는 중요한 정보를 제공할 수 있습니다.

식별: 방화벽 액세스 목록 Syslog 메시지

log 키워드가 없는 ACE(Access Control Entry)에서 거부된 패킷에 대해 방화벽 syslog 메시지 **106023**이 생성됩니다. 이 syslog 메시지에 대한 추가 정보는 Cisco ASA 5500 Series System Log Message, 8.2 - 106023에 있습니다.

Cisco ASA 5500 Series Adaptive Security Appliance용 syslog 구성에 대한 정보는 Monitoring - Configuring Logging에 있습니다. Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터에 대한 FWSM의 syslog 구성에 대한 정보는 Monitoring the Firewall Services Module에 있습니다.

다음 예에서는 **show logging | grep** *regex* 명령은 방화벽의 로깅 버퍼에서 syslog 메시지를 추출합니다. 이러한 메시지는 본 문서에 설명된 취약성을 악용하려는 잠재적 시도를 나타낼 수 있는 거부된 패킷에 대한 추가 정보를 제공합니다. 로깅된 메시지에서 특정 데이터를 검색하기 위해 **grep** 키워드와 다른 정규식을 사용할 수 있습니다.

정규식 구문에 대한 추가 정보는 정규식 만들기에 있습니다.

```
firewall#show logging | grep 106023
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.194/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.164/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.106/23 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.241/23 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.169/1025
 dst inside:192.168.60.56/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.36/1025
 dst inside:192.168.60.202/22 by access-group "tACL-Policy"
firewall#
```

앞의 예에서 tACL tACL-Policy에 대해 로깅된 메시지에는 TCP 포트 **22**에 대한 SSH 패킷과 TCP 포트 23**에** 대한 텔넷 패킷이 **인프라 디바이스에 할당된 주소 블록으로 전송되는 것이** 표시됩니다.

ASA 보안 어플라이언스용 syslog 메시지에 대한 추가 정보는 Cisco ASA 5500 Series System Log Messages, 8.2에 있습니다. FWSM용 syslog 메시지에 대한 추가 정보는 Catalyst 6500 Series Switch 및 Cisco 7600 Series Router Firewall Services Module Logging System Log Messages에 있습니다.

syslog 이벤트를 사용한 인시던트 조사에 대한 자세한 내용은 Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence 백서를 참조하십시오.

추가 정보

개정 이력

개정 1.0	2011년 6월 1일	초기 공개

Cisco 보안 절차

Cisco 제품의 보안 취약성 보고, 보안 사고에 대한 지원 요청, Cisco의 보안 정보 수신을 위한 등록 등에 대한 자세한 내용은 Cisco의 전 세계 웹 사이트 (https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html)에서 확인할 수 있습니다. 여기에는 Cisco 보안 알림과 관련된 언론 문의에 대한 지침이 포함됩니다. 모든 Cisco 보안 권고 사항은 http://www.cisco.com/go/psirt에서 확인할 수 있습니다.

관련 정보

- Cisco Applied Mitigation 게시판
- Cisco 보안
- Cisco Security IntelliShield Alert Manager Service
- Cisco IOS 디바이스를 강화하는 Cisco 가이드
- Cisco IOS NetFlow - 홈 페이지(Cisco.com)

- Cisco IOS NetFlow 백서
- NetFlow 성능 분석
- Cisco 네트워크 기반 보호 백서
- Cisco Network Foundation Protection 프레젠테이션
- TTL 만료 공격 식별 및 완화
- 보안 중심의 IP 주소 지정 방식
- IPv6 Type 0 라우팅 헤더의 악의적인 사용에 대한 대책
- Cisco IOS의 보안 툴 명령 언어
- Cisco 방화벽 제품 - 홈 페이지 Cisco.com
- CVE(Common Vulnerabilities and Exposures)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.