Cisco Content Services Gateway Denial of Service 취약성 식별 및 완화

Cisco Content Services Gateway Denial of Service 취약성 식별 및 완화

자문 ID: cisco-amb-20110706-csg

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110706-csg

개정 1.0

2011년 7월 6일 16:00 UTC(GMT) 공개 릴리스의 경우

목차

Cisco의 대응

이 Applied Mitigation Bulletin은 PSIRT Security Advisory *Cisco Content Services Gateway Denial of Service Vulnerability*에 대한 설명서이며 관리자가 Cisco 네트워크 디바이스에 구축할 수 있는 식별 및 완화 기술을 제공합니다.

취약성 특성

Cisco CSG2(Content Services Gateway - Second Generation)에는 특별히 고안된 일련의 ICMP 패킷을 처리할 때 취약성이 포함되어 있습니다. 이 취약성은 인증 없이, 그리고 최종 사용자 상호 작용 없이 원격으로 악용될 수 있습니다. 이 취약성을 성공적으로 악용하면 영향을 받는 디바이스가 다시 로드되어 DoS(서비스 거부) 상태가 될 수 있습니다. 이 취약성을 악용하려는 시도가 반복되면 DoS 상태가 지속될 수 있습니다. 익스플로잇을 위한 공격 벡터는 일련의 ICMP 패킷을 통해 이루어집니다.

이 취약성에는 CVE 식별자 CVE-2011-2064가 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 있습니다. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

20110706-csg

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 tACL(transit 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 IPS(Intrusion Prevention System) 이벤트 작업을 효과적으로 사용하면 이 취약성을 악용하려는 공격에 대한 가시성과 차단 기능을 제공할 수 있습니다.

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

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

Cisco Security MARS(Monitoring, Analysis, and Response System) 어플라이언스는 사고, 쿼리 및 이벤트 보고를 통해 가시성을 제공할 수도 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 침입 방지 시스템
- Cisco 보안 모니터링, 분석 및 대응 시스템

Cisco IOS 라우터 및 스위치

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 tACL(transit access control list)을 구축하여 정책 시행을 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 에코 요청, 에코 응답, 호스트 도달 불가, 추적 경로, 패킷 너무 큼, 시간 초과, 도달 불가 등의 무단 ICMP 패킷 유형을 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 protocol ! access-list 150 permit icmp host 192.168.100.1
192.168.60.0 0.0.0.255 echo access-list 150 permit icmp host 192.168.100.1
192.168.60.0 0.0.0.255 echo-reply access-list 150 permit icmp host 192.168.100.1
192.168.60.0 0.0.0.255 host-unreachable access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 traceroute access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 packet-too-big access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 time-exceeded access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 unreachable ! !-- The following vulnerability-
specific access control entries !-- (ACEs) can aid in identification of attacks !
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 echo access-list 150 deny icmp
any 192.168.60.0 0.0.0.255 echo-reply access-list 150 deny icmp any 192.168.60.0
0.0.0.255 host-unreachable access-list 150 deny icmp any 192.168.60.0 0.0.0.255
traceroute access-list 150 deny icmp any 192.168.60.0 0.0.0.255 packet-too-big
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 time-exceeded access-list 150
deny icmp any 192.168.60.0 0.0.0.255 unreachable ! !-- 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 150 deny ip
any any ! !-- Apply tACL to interfaces in the ingress direction ! interface
GigabitEthernet0/0 ip access-group 150 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:트랜짓 액세스 제어 목록

관리자가 인터페이스에 tACL을 적용한 후 **show ip access-lists 명령**은 필터링된 에코 요청, 에코 응답, host-unreachable, traceroute, packet-too-big, time-exceeded, unreachable을 비롯한 ICMP 패킷 유형의 수를 식별합니다. 관리자는 필터링된 패킷을 조사하여 이 취약성을 악용하려는 시도인지

확인하는 것이 좋습니다. **show ip access-lists 150**에 대한 **출력의 예**는 다음과 같습니다.

```
router#show ip access-lists 150
Extended IP access list 150
    10 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo
    20 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo-reply
    30 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 host-unreachable
    40 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 traceroute
    50 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 packet-too-big
    60 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 time-exceeded
    70 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 unreachable
    80 deny icmp any 192.168.60.0 0.0.0.255 echo (12 matches)
    90 deny icmp any 192.168.60.0 0.0.0.255 echo-reply (26 matches)
    100 deny icmp any 192.168.60.0 0.0.0.255 host-unreachable (10 matches)
    110 deny icmp any 192.168.60.0 0.0.0.255 traceroute (7 matches)
    120 deny icmp any 192.168.60.0 0.0.0.255 packet-too-big (9 matches)
    130 deny icmp any 192.168.60.0 0.0.0.255 time-exceeded (2 matches)
    140 deny icmp any 192.168.60.0 0.0.0.255 unreachable (18 matches)
    150 deny ip any any
router#
```

앞의 예에서 액세스 목록 150은 신뢰할 수 없는 호스트 또는 네트워크로부터 수신한 다음 패킷을 삭제했습니다.

- ACE 라인 80에 대한 **12개 ICMP 에코 요청** 패킷
- ACE 라인 90**에** 대한 **26**개의 **ICMP 에코 응답** 패킷
- ACE 라인 100**에** 대한 **ICMP 호스트** 도달 불가 패킷 **10개**
- ACE 라인 110용 **ICMP** 트레이스라우트 패킷 **7개**
- ACE 라인 120**에** 대한 **ICMP** 패킷**-too-big** 패킷 **9개**
- ACE 라인 130**에** 대한 **2**개의 **ICMP 시간 초과** 패킷
- ACE 라인 140**에** 대한 **18**개의 **ICMP** 도달 불가 패킷

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.

ID: 액세스 목록 로깅

log and **log-input** ACL(access control list) 옵션을 사용하면 특정 ACE와 일치하는 패킷이 로깅됩니다. **log-input 옵션**은 패킷 소스 및 목적지 IP 주소와 포트 외에 인그레스 인터페이스의 로깅을 활성화합니다.

주의: 액세스 제어 목록 로깅은 CPU를 많이 사용할 수 있으므로 각별한 주의를 기울여 사용해야 합니다. ACL 로깅의 CPU 영향을 제어하는 요소는 로그 생성, 로그 전송, 로그 지원 ACE와 일치하는 패킷을 전달하는 프로세스 스위칭입니다.

Cisco IOS Software의 경우 **ip access-list logging interval** *in-ms 명령은* ACL 로깅에 의해 유발되는 프로세스 전환의 효과를 제한할 수 있습니다. logging **rate-limit** *rate-per-second* [**except** *loglevel*] 명령은 로그 생성 및 전송의 영향을 제한합니다.

ACL 로깅의 CPU 영향은 Supervisor Engine 720 또는 Supervisor Engine 32를 사용하는 Cisco Catalyst 6500 Series 스위치와 Cisco 7600 Series 라우터의 하드웨어에서 최적화된 ACL 로깅을 사

용하여 해결할 수 있습니다.

ACL 로깅의 컨피그레이션 및 사용에 대한 자세한 내용은 ACL 로깅 적용 인텔리전스 이해 백서를 참조하십시오.

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 (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  0 active, 16384 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-Telnet    11393421      2.8         1    48      3.1       0.0       1.4
TCP-FTP            236      0.0        12    66      0.0       1.8       4.8
TCP-FTPD            21      0.0     13726  1294      0.0      18.4       4.1
TCP-WWW          22282      0.0        21  1020      0.1       4.1       7.3
TCP-X              719      0.0         1    40      0.0       0.0       1.3
TCP-BGP              1      0.0         1    40      0.0       0.0      15.0
TCP-Frag         70399      0.0         1   688      0.0       0.0      22.7
TCP-other     47861004     11.8         1   211     18.9       0.0       1.3
UDP-DNS            582      0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957     14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  01 0984 0800     9
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  01 0911 0000     4
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   01 0B3E 0301     5
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   01 0B89 0030     1
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  01 0BD7 0200     7
```

```
Gi0/0          192.168.15.130  Gi0/1          192.168.60.239  01 0BD7 1100     3
Gi0/0          192.168.23.220  Gi0/1          192.168.60.239  01 0BD7 0300    11
Gi0/0          10.89.16.226    Gi0/1          192.168.150.60  06 12CA 0016     1
router#
```

앞의 예에서는 **ICMP 에코 요청(16진수 값 0800), echo-reply(16진수 값 0000), host-unreachable(16진수 값 0301), traceroute(16진수 값 0030), packet-too-big(16진수 값 0200), time-exceeded(16진수 값 1100) 및 unreachable(16진수 값 0300) ICMP** 패킷 유형에 대한 여러 흐름이 있습니다.

앞서 언급한 ICMP 패킷 유형에 대한 트래픽 흐름만 보려면 명령을 **show ip cache flow로 실행합니다 | include SrcIf| _01_.*(0800|0000|0301|0030|0200|1100|0300)_는** 다음 그림과 같이 관련 ICMP NetFlow 레코드를 표시합니다.

ICMP 흐름

```
router#show ip cache flow | include SrcIf|_01_.*(0800|0000|0301|0030|0200|1100|0300)_
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0          192.168.10.201  Gi0/1          192.168.60.102  01 0984 0800     9
Gi0/0          192.168.11.54   Gi0/1          192.168.60.158  01 0911 0000     4
Gi0/0          192.168.13.97   Gi0/1          192.168.60.28   01 0B3E 0301     5
Gi0/0          192.168.10.17   Gi0/1          192.168.60.97   01 0B89 0030     1
Gi0/0          192.168.12.185  Gi0/1          192.168.60.239  01 0BD7 0200     7
Gi0/0          192.168.15.130  Gi0/1          192.168.60.239  01 0BD7 1100     3
Gi0/0          192.168.23.220  Gi0/1          192.168.60.239  01 0BD7 0300    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 에코 요청, 에코 응답, 호스트 도달 불가, 추적 경로, 패킷 너무 큼, 시간 초과, 도달 불가 등의 무단 ICMP 패킷 유형을 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 protocol ! access-list tACL-Policy extended permit icmp host
192.168.100.1 192.168.60.0 255.255.255.0 echo access-list tACL-Policy extended permit
icmp host 192.168.100.1 192.168.60.0 255.255.255.0 echo-reply access-list tACL-Policy
extended permit icmp host 192.168.100.1 192.168.60.0 255.255.255.0 traceroute access-
list tACL-Policy extended permit icmp host 192.168.100.1 192.168.60.0 255.255.255.0 2
access-list tACL-Policy extended permit icmp host 192.168.100.1 192.168.60.0
```

```
255.255.255.0 time-exceeded access-list tACL-Policy extended permit icmp host
192.168.100.1 192.168.60.0 255.255.255.0 unreachable ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in identification of
attacks ! access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
echo access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0 echo-
reply access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
traceroute access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
2 access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0 time-
exceeded access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
unreachable ! !-- 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 적용되면 관리자는 **show access-list 명령**을 사용하여 에코 요청, 에코 응답, 호스트 도달 불가, 추적 가능, 패킷 너무 큼, 시간 초과, 도달 불가 등 필터링된 ICMP 패킷 유형의 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; 13 elements
access-list tACL-Policy line 1 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 echo
access-list tACL-Policy line 2 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 echo-reply
access-list tACL-Policy line 3 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 traceroute
access-list tACL-Policy line 4 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 2
access-list tACL-Policy line 5 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 time-exceeded
access-list tACL-Policy line 6 extended permit icmp host 192.168.100.1
     192.168.60.0 255.255.255.0 unreachable
access-list tACL-Policy line 7 extended deny icmp any
     192.168.60.0 255.255.255.0 echo (hitcnt=9)
access-list tACL-Policy line 8 extended deny icmp any
     192.168.60.0 255.255.255.0 echo-reply (hitcnt=12)
access-list tACL-Policy line 9 extended deny icmp any
     192.168.60.0 255.255.255.0 traceroute (hitcnt=7)
access-list tACL-Policy line 10 extended deny icmp any
     192.168.60.0 255.255.255.0 2 (hitcnt=11)
access-list tACL-Policy line 11 extended deny icmp any
     192.168.60.0 255.255.255.0 time-exceeded (hitcnt=5)
access-list tACL-Policy line 12 extended deny icmp any
     192.168.60.0 255.255.255.0 unreachable (hitcnt=8)
access-list tACL-Policy line 13 extended deny ip any any (hitcnt=17)
fireall#
```

앞의 예에서 액세스 목록 tACL-*Policy*는 신뢰할 수 없는 호스트 또는 네트워크에서 받은 다음 패킷을 삭제했습니다.

- ACE 라인 7에 대한 **ICMP 에코** 패킷 **9개**
- ACE 라인 8**에** 대한 **12**개의 **ICMP 에코 응답** 패킷
- ACE 라인 9용 **ICMP** 트레이스라우트 패킷 **7**개
- ACE 라인 10**에** 대한 **ICMP** 패킷**-too-big** 패킷 **11개**

- ACE 라인 11에 대한 **ICMP 시간 초과** 패킷 **5개**
- ACE 라인 12**에** 대한 **8개**의 **ICMP 연결 불가** 패킷

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
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/2048 by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.2.0.200/2945
         dst inside:192.168.60.33/0 by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.99/2946
         dst inside:192.168.60.240/48 by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.100/2947
         dst inside:192.168.60.115/512 by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.88/2949
         dst inside:192.168.60.38/4352  by access-group "tACL-Policy"
  Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.175/2950
         dst inside:192.168.60.250/768 by access-group "tACL-Policy"
firewall#
```

앞의 예에서 tACL tACL *정책*에 대해 로깅된 메시지는 **ICMP** 패킷 유형 **에코 요청, 에코 응답, traceroute, packet-too-big, time-exceeded, unreachable이 영향을** 받은 디바이스에 할당된 주소 블록으로 전송됨을 보여줍니다.

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.

Cisco 침입 방지 시스템

완화: Cisco IPS 서명 이벤트 작업

관리자는 Cisco IPS(Intrusion Prevention System) 어플라이언스 및 서비스 모듈을 사용하여 위협 탐지를 제공하고 이 문서에 설명된 취약성을 악용하려는 시도를 방지할 수 있습니다. Cisco IPS 버

전 6.x 이상을 실행하는 센서에 대한 시그니처 업데이트 S580부터 시그니처 38247/0(시그니처 이름: Cisco Content Services Gateway Denial of Service)으로 취약성을 탐지할 수 있습니다. 시그니처 38247/0은 기본적으로 활성화되어 *중간* 심각도 이벤트를 트리거하고 SFR(Signature Fidelity Rating)이 90이며 기본 이벤트 작업인 **produce-alert**로 **구성됩니다**.

Signature 38247/0은 ICMP를 사용하여 전송된 여러 패킷이 감지될 때 발생합니다. 이 서명의 실행은 취약성의 잠재적인 익스플로잇을 나타낼 수 있습니다.

관리자는 공격이 탐지될 때 이벤트 작업을 수행하도록 Cisco IPS 센서를 구성할 수 있습니다. 구성된 이벤트 작업은 이 문서에 설명된 취약성을 악용하려는 공격에 대해 보호할 수 있도록 예방 또는 억제 제어를 수행합니다.

Cisco IPS 센서는 이벤트 동작의 사용과 결합된 인라인 보호 모드에서 구축될 때 가장 효과적입니다. 인라인 보호 모드에서 구축된 Automatic Threat Prevention for Cisco IPS 6.x 이상 센서는 이 문서에 설명된 취약성을 악용하려는 공격에 대한 위협 방지 기능을 제공합니다. 위협 방지는 riskRatingValue가 90보다 큰 트리거된 서명에 대해 이벤트 작업을 수행하는 *기본 재정의*를 통해 구현됩니다.

위험 등급 및 위협 등급 계산에 대한 자세한 내용은 위험 등급 및 위협 등급: IPS 정책 관리 간소화를 참조하십시오.

Cisco 보안 모니터링, 분석 및 대응 시스템

식별: Cisco 보안 모니터링, 분석 및 대응 시스템 사고

Cisco Security MARS(Monitoring, Analysis, and Response System) 어플라이언스는 IPS 서명 38247/0(서명 이름: Cisco Content Services Gateway Denial of Service)을 사용하여 이 문서에 설명된 취약성과 관련된 이벤트와 관련된 인시던트를 생성할 수 있습니다. S580 동적 서명 업데이트가 다운로드된 후 키워드 **NR-38247/0** for IPS signature 38247/0 및 Cisco Security MARS 어플라이언스의 **All Matching Events** 쿼리 유형을 사용하여 IPS 서명에 의해 생성된 인시던트를 나열하는 보고서를 제공합니다.

Cisco Security MARS 어플라이언스의 4.3.1 및 5.3.1 릴리스부터 Cisco IPS 동적 서명 업데이트 기능에 대한 지원이 추가되었습니다. 이 기능은 Cisco.com 또는 로컬 웹 서버에서 새 서명을 다운로드하고, 해당 서명과 일치하는 수신된 이벤트를 정확하게 처리 및 분류하며, 이를 검사 규칙 및 보고서에 포함합니다. 이러한 업데이트는 이벤트 표준화 및 이벤트 그룹 매핑을 제공하며 MARS 어플라이언스에서 IPS 디바이스의 새 서명을 구문 분석할 수 있게 합니다.

주의: 동적 서명 업데이트가 구성되지 않은 경우 이러한 새 서명과 일치하는 이벤트는 쿼리와 보고서에서 *알 수 없는 이벤트* 유형으로 표시됩니다. MARS는 이러한 이벤트를 검사 규칙에 포함하지 않으므로 네트워크 내에서 발생하는 잠재적인 위협이나 공격에 대한 인시던트가 생성되지 않을 수 있습니다.

기본적으로 이 기능은 활성화되어 있지만 컨피그레이션이 필요합니다. 구성되지 않은 경우 다음 Cisco 보안 MARS 규칙이 트리거됩니다.

```
System Rule: CS-MARS IPS Signature Update Failure
```

이 기능을 활성화하고 구성하면 관리자는 **도움말 > 정보**를 선택하고 *IPS 서명 버전 값*을 검토하여 MARS에서 다운로드한 현재 서명 버전을 결정할 수 있습니다.

동적 서명 업데이트에 대한 추가 정보 및 동적 서명 업데이트 구성에 대한 지침은 Cisco Security

MARS 4.3.1 및 5.3.1 릴리스에 제공됩니다.

추가 정보

이 문서는 "있는 그대로" 제공되며, 상품성 또는 특정 사용에 대한 적합성의 보증을 포함하여 어떤 종류의 보장 또는 보증도 의미하지 않습니다. 문서 또는 문서에 링크된 자료의 정보를 사용하는 것은 귀하의 책임입니다. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

개정 이력

개정 1.0	2011년 7월 6일	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
- 보안 중심의 IP 주소 지정 방식
- 컨트롤 플레인 보호 이해
- Cisco IOS의 보안 툴 명령 언어
- Cisco 방화벽 제품 - 홈 페이지 Cisco.com
- Cisco 침입 방지 시스템
- Cisco IPS 서명 다운로드
- Cisco IPS 서명 검색 페이지
- Cisco 보안 모니터링, 분석 및 대응 시스템
- 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.