Identificatie en beperking van exploitatie van de kwetsbaarheid van Cisco Content Services Gateway voor Denial of Service

Identificatie en beperking van exploitatie van de kwetsbaarheid van Cisco Content Services Gateway voor Denial of Service

Advies-ID: cisco-amb-20110706-csg

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

Revisie 1.0

2011 juli 6 16:00 UTC (GMT)

Inhoud

Cisco Response

Dit Toegepaste Matiging Bulletin is een begeleidend document bij de kwetsbaarheid voor *contentservices gateway Denial of Service van* PSIRT Security Advisory *van Cisco* en biedt identificatie- en mitigatietechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

Cisco Content Services Gateway - Second Generation (CSG2) bevat een kwetsbaarheid bij het verwerken van een reeks speciaal vervaardigde ICMP-pakketten. Deze kwetsbaarheid kan op afstand worden benut zonder authenticatie en zonder interactie van de eindgebruiker. Een succesvolle benutting van deze kwetsbaarheid kan ervoor zorgen dat het betreffende apparaat opnieuw wordt geladen, wat kan resulteren in een DoS-conditie (Denial of Service). Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie. De aanvalsvector voor exploitatie is door een reeks ICMP-pakketten.

Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-2064.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory, die beschikbaar is via de volgende link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110706-csg.

Overzicht Mitigation Technique

Cisco-apparaten bieden verschillende tegenmaatregelen voor deze kwetsbaarheid. Beheerders wordt aangeraden deze beveiligingsmethoden te beschouwen als algemene best practices op het gebied van beveiliging van infrastructuurapparaten en het verkeer dat het netwerk doorkruist. In dit gedeelte van het document wordt een overzicht van deze technieken gegeven.

Cisco IOS-software kan effectieve middelen voor explosiepreventie bieden door gebruik te maken van transittoegangscontrolelijsten (tACL's).

Dit beschermingsmechanisme filtert en laat pakketten vallen die proberen deze kwetsbaarheid te exploiteren.

Effectieve explosiepreventie kan ook worden geboden door de Cisco ASA 5500 Series adaptieve security applicatie en de Firewall Services Module (FWSM) voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers die gebruikmaken van doorvoertoegangscontrolelijsten (tACL's).

Dit beschermingsmechanisme filtert en laat pakketten vallen die proberen deze kwetsbaarheid te exploiteren.

Effectief gebruik van de gebeurtenisacties van Cisco Inbraakpreventiesysteem (IPS) biedt zichtbaarheid in en bescherming tegen aanvallen die proberen deze kwetsbaarheid te exploiteren.

Cisco IOS NetFlow-records kunnen zichtbaarheid bieden in netwerkgebaseerde exploitatiepogingen.

Cisco IOS-software, Cisco ASA en FWSM firewalls kunnen zichtbaarheid bieden door syslog-berichten en tegenwaarden die worden weergegeven in de uitvoer van **show-**opdrachten.

Het Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) applicatie kan ook zichtbaarheid bieden via incidenten, vragen en gebeurtenisrapportage.

Risicobeheer

Organisaties wordt aangeraden hun standaardprocessen voor risicobeoordeling en risicobeperking te volgen om de mogelijke gevolgen van deze kwetsbaarheid te bepalen. Triage verwijst naar het sorteren van projecten en het prioriteren van inspanningen die waarschijnlijk het meest succesvol zullen zijn. Cisco heeft documenten geleverd die organisaties kunnen helpen bij de ontwikkeling van een op risico gebaseerde triagecapaciteit voor hun informatieveiligheidsteams. Risico Triage voor Security Vulnerability aankondigingen en Risk Triage en Prototyping kunnen organisaties helpen herhaalbare security evaluatie- en reactieprocessen te ontwikkelen.

Apparaatspecifieke beperking en identificatie

Waarschuwing: de effectiviteit van elke mitigatietechniek hangt af van specifieke klantsituaties, zoals productmix, netwerktopologie, verkeersgedrag en organisatorische missie. Zoals bij elke configuratiewijziging, evalueer het effect van deze configuratie voordat u de wijziging toepast.

Voor deze hulpmiddelen is specifieke informatie over beperking en identificatie beschikbaar:

- Cisco IOS-routers en -Switches
- Cisco IOS NetFlow
- Cisco ASA- en FWSM-firewalls
- Cisco-inbraakpreventiesysteem
- Cisco-systeem voor beveiligingsbewaking, analyse en respons

Cisco IOS-routers en -Switches

Beperking: toegangscontrolelijsten voor douanevervoer

Om het netwerk te beschermen tegen verkeer dat het netwerk ingaat op toegangspunten, die internetverbindingspunten, partner- en leverancierspunten of VPN-verbindingspunten kunnen omvatten, wordt beheerders aangeraden om transittoegangscontrolelijsten (tACL's) te implementeren om beleidshandhaving uit te voeren. Beheerders kunnen een tACL construeren door alleen geautoriseerd verkeer expliciet toe te staan om het netwerk op access points binnen te gaan of door geautoriseerd verkeer toe te staan om door het netwerk te reizen in overeenstemming met bestaand beveiligingsbeleid en configuraties. Een tACL-tijdelijke oplossing kan geen volledige bescherming tegen deze kwetsbaarheid bieden wanneer de aanval afkomstig is van een vertrouwd bronadres.

Het tACL-beleid ontkent onbevoegde ICMP-pakkettypen, waaronder echoverzoek, echo-antwoord, host-onbereikbaar, traceroute, packet-to-big, time-violation en onbereikbaar, die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 is de IP adresruimte die door de beïnvloede apparaten wordt gebruikt, en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend.

Aanvullende informatie over tACL's staat in Transit Access Control Lists: Filtering at Your Edge.

```
! !-- 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
```

Merk op dat het filtreren met een lijst van de interfacetoegang de transmissie van onbereikbare berichten ICMP terug naar de bron van het gefilterde verkeer zal veroorzaken. Het genereren van deze berichten zou het ongewenste effect kunnen hebben van het verhogen van CPU-gebruik op het apparaat. In Cisco IOS-software is de onbereikbare ICMP-generatie standaard beperkt tot één pakket per 500 milliseconden. ICMP onbereikbare berichtgeneratie kan worden uitgeschakeld met de opdracht interfaceconfiguratie **zonder IP-onbereikbaar**. ICMP-onbereikbare snelheidsbeperking kan worden gewijzigd ten opzichte van de standaardinstelling met behulp van de **algemene** opdracht voor configuratie **ip icmp-snelheidslimiet voor onbereikbare** *interval-in-ms*.

Identificatie:Toegangscontrolelijsten voor douanevervoer

Nadat de beheerder tACL op een interface heeft toegepast, zal de opdracht **IP-toegangslijsten tonen** het aantal ICMP-pakkettypen identificeren, inclusief echoverzoek, echoantwoord, host-onbereikbaar, traceroute, packet-to-big, time-violation en onbereikbaar, die zijn gefilterd. De beheerders worden geadviseerd om gefilterde pakketten te onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont ip toegang-lijsten 150** volgt:

```
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#
```

In het voorafgaande voorbeeld, heeft toegangslijst 150 de volgende pakketten gelaten vallen die van een onbetrouwbare gastheer of een netwerk worden ontvangen:

- **12 ICMP-**echoverdrachtpakketten voor ACE-lijn 80
- **26 ICMP-**pakketten **voor echo-antwoord** voor ACE-lijn 90
- **10 ICMP host-onbereikbare** pakketten voor ACE-lijn 10
- **7 ICMP traceroute-**pakketten voor ACE-lijn 110
- **9 ICMP-pakketto-grote** pakketten voor ACE-lijn 120
- **2 ICMP-**pakketten **met tijdoverschrijding** voor ACE-lijn 130
- **18 ICMP onbereikbare** pakketten voor ACE-lijn 140

Voor extra informatie over het onderzoeken van incidenten met ACE-tellers en syslog-gebeurtenissen, raadpleegt u het white paper Identifying Incidents Use Firewall en IOS Router

Syslog Events Applied Intelligence.

Beheerders kunnen Embedded Event Manager gebruiken om instrumentatie te bieden wanneer aan specifieke voorwaarden is voldaan, zoals ACE-tellers. De Applied Intelligence white paper Embedded Event Manager in een security context biedt aanvullende informatie over hoe deze functie te gebruiken.

Identificatie: Vastlegging toegangslijst

De optie **log** en **log-input** toegangscontrolelijst (ACL) zorgt ervoor dat pakketten die overeenkomen met specifieke ACE's worden vastgelegd. De **log-**inputoptie maakt het registreren van de toegangsinterface mogelijk, naast de IP-adressen en -poorten van de pakketbron en de bestemming.

Waarschuwing: vastlegging in toegangscontrolelijst kan zeer CPU-intensief zijn en moet met uiterste voorzichtigheid worden gebruikt. De factoren die de CPU-impact van ACL-vastlegging bepalen, zijn loggeneratie, logtransmissie en processwitching naar voorwaartse pakketten die logbestanden met ACE's matchen.

Voor Cisco IOS-software kan de opdracht **interval**-*in-ms* **vastlegging van IP-toegangslijst** de effecten van processwitching beperken die worden geïnduceerd door ACL-vastlegging. De **logsnelheid-limiet** *rate-per-seconde* [**behalve** *loglevel*] opdracht beperkt het effect van loggeneratie en transmissie.

De CPU-impact van ACL-vastlegging kan worden aangepakt in hardware op de Cisco Catalyst 6500 Series-switches en Cisco 7600 Series-routers met Supervisor Engine 720 of Supervisor Engine 32 met behulp van geoptimaliseerde ACL-vastlegging.

Voor extra informatie over de configuratie en het gebruik van ACL-vastlegging raadpleegt u het Witboek Inzicht in toegangscontrolelijst en toegepaste intelligentie.

Cisco IOS NetFlow

Identificatie: Traffic Flow Identification met NetFlow-records

Beheerders kunnen Cisco IOS NetFlow configureren op Cisco IOS-routers en -switches om te helpen bij de identificatie van verkeersstromen die pogingen kunnen zijn om de kwetsbaarheid te exploiteren. De beheerders worden geadviseerd om stromen te onderzoeken om te bepalen of zij pogingen zijn om de kwetsbaarheid te exploiteren of of zij wettige verkeersstromen zijn.

```
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#
```

In het bovenstaande voorbeeld zijn er meerdere stromen voor de volgende **ICMP-**pakkettypen: **ICMP-echoverzoek (hex-waarde 0800), echo-antwoord (hex-waarde 0000), host-onbereikbaar (hex-waarde 0301), traceroute (hex-waarde 0030), packet-to-big (hex-waarde 0200), time-beyond (hex-waarde 1100) en onbereikbaar (hex-waarde 0300)**.

Als u alleen de verkeersstromen voor de bovengenoemde ICMP-pakkettypen wilt weergeven, **toont** de opdracht **de IP-cachedoorvoer | omvat SrcIf|_01_.*(0800|000|0301|0030|0200|1100|0300)_** de gerelateerde ICMP NetFlow-records zal weergeven zoals hieronder wordt getoond:

ICMP-stromen

```
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- en FWSM-firewalls

Beperking: toegangscontrolelijsten voor douanevervoer

Om het netwerk te beschermen tegen verkeer dat het netwerk ingaat op toegangspunten die internetverbindingspunten, partner- en leverancierverbindingen of VPN-verbindingspunten kunnen omvatten, wordt beheerders aangeraden om tACL's te implementeren om beleidshandhaving uit te voeren. Beheerders kunnen een tACL construeren door alleen geautoriseerd verkeer expliciet toe te staan om het netwerk op access points binnen te gaan of door geautoriseerd verkeer toe te staan om door het netwerk te reizen in overeenstemming met bestaand beveiligingsbeleid en configuraties. Een tACL-tijdelijke oplossing kan geen volledige bescherming tegen deze kwetsbaarheid bieden wanneer de aanval afkomstig is van een vertrouwd bronadres.

Het tACL-beleid ontkent onbevoegde ICMP-pakkettypen, waaronder echoverzoek, echo-antwoord, host-onbereikbaar, traceroute, packet-to-big, time-violation en onbereikbaar, die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 is de IP adresruimte die door de beïnvloede apparaten wordt gebruikt, en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend.

Aanvullende informatie over tACL's staat in Transit Access Control Lists: Filtering at Your Edge.

```
! !-- 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
```

Identificatie: Toegangscontrolelijsten voor douanevervoer

Nadat tACL is toegepast op een interface, kunnen de beheerders het bevel gebruiken van de **show toegang-lijst** om het aantal pakkettypes ICMP met inbegrip van echoverzoek, echo-antwoord, gastheer-onbereikbaar, traceroute, pakket-te-groot, tijd-overschreden, en onbereikbaar te identificeren, die zijn gefilterd. De beheerders worden geadviseerd om gefilterde pakketten te onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont toegang-lijst aan ACL-Beleid** volgt:

```
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#
```

In het voorafgaande voorbeeld, heeft de toegangslijst *tACL-Policy* de volgende pakketten die van een onbetrouwbare host of een onbetrouwbaar netwerk zijn ontvangen, verbroken:

- **9 ICMP-**echopakketten voor ACE-lijn 7
- **12 ICMP-**pakketten **voor echo-antwoord** voor ACE-lijn 8
- **7 ICMP traceroute-**pakketten voor ACE-lijn 9
- **1 ICMP-pakketto-grote** pakketten voor ACE-lijn 10
- **5 ICMP-**pakketten **met tijdoverschrijding** voor ACE-lijn 11
- **8 ICMP onbereikbare** pakketten voor ACE-lijn 12

Identificatie: berichten in Firewall Access List System

Firewallsyslog-bericht *106023* wordt gegenereerd voor pakketten die worden geweigerd door een toegangscontrole-ingang (ACE) die niet het trefwoord voor het **logbestand** heeft. Aanvullende informatie over dit syslogbericht wordt weergegeven in Cisco ASA 5500 Series systeemlogbericht, 8.2 - 106023.

Informatie over het configureren van syslog voor de Cisco ASA 5500 Series adaptieve security applicatie is beschikbaar in Monitoring - Configuration Logging. De informatie over het configureren van syslog op de FWSM voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers is beschikbaar in Monitoring the Firewall Services Module.

In het volgende voorbeeld, de **show vastlegging | grep** *regex* opdracht haalt syslog berichten uit de logboekbuffer op de firewall. Deze berichten verstrekken extra informatie over ontkende pakketten die op potentiële pogingen zouden kunnen wijzen om de kwetsbaarheid te exploiteren die in dit document wordt beschreven. Het is mogelijk om verschillende reguliere expressies te gebruiken met het **grep**-sleutelwoord om te zoeken naar specifieke gegevens in de geregistreerde berichten.

Aanvullende informatie over de syntaxis van reguliere expressies is te vinden in Create a Regular Expression.

```
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#
```

In het vorige voorbeeld, tonen de berichten die voor het tACL *tACL-Policy* worden geregistreerd **ICMP** pakkettypes **echoverzoek, echo-antwoord, traceroute, pakket-to-big, tijd-overschreden, en onbereikbaar** verzonden naar het adresblok dat aan beïnvloede apparaten wordt toegewezen.

Aanvullende informatie over syslogberichten voor ASA-beveiligingsapparaten is te vinden in Cisco ASA 5500 Series systeemlogberichten, 8.2. Aanvullende informatie over syslog-berichten voor de FWSM is te vinden in Catalyst 6500 Series Switch en Cisco 7600 Series router Firewall Services Module Logging System Berichten.

Voor extra informatie over het onderzoeken van incidenten met behulp van syslog-gebeurtenissen, raadpleegt u het white paper Identifying Incidents Using Firewall en IOS Router Syslog Events Applied Intelligence.

Cisco-inbraakpreventiesysteem

Beperken: acties voor Cisco IPS-handtekeningen

Beheerders kunnen Cisco Inbraakpreventiesysteem (IPS) gebruiken om bedreigingsdetectie te bieden en pogingen te voorkomen om de kwetsbaarheid te exploiteren die in dit document wordt beschreven. Beginnend met handtekeningsupdate S580 voor sensoren waarop Cisco IPS versie 6.x en hoger wordt uitgevoerd, kan de kwetsbaarheid worden gedetecteerd door handtekening 38247/0 (Handtekeningnaam: Cisco Content Services Gateway Denial of Service). Signature 38247/0 is standaard ingeschakeld, activeert een *Medium* Severity event, heeft een Signature Fidelity Rating (SFR) van 90 en is geconfigureerd met een default event action of **production-alert**.

Vuren van handtekening 38247/0 wanneer meerdere pakketten worden verzonden met ICMP worden gedetecteerd. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van de kwetsbaarheid.

Beheerders kunnen Cisco IPS-sensoren configureren om een gebeurtenisactie uit te voeren wanneer een aanval wordt gedetecteerd. De geconfigureerde gebeurtenisactie voert preventieve of afschrikkende controles uit om te helpen beschermen tegen een aanval die probeert de kwetsbaarheid te exploiteren die in dit document wordt beschreven.

Cisco IPS-sensoren zijn het meest effectief wanneer ze worden ingezet in inline beschermingsmodus in combinatie met het gebruik van een gebeurtenisactie. Automatische

bedreigingspreventie voor Cisco IPS 6.x en grotere sensoren die in de modus voor inline bescherming worden geïmplementeerd, biedt bedreigingspreventie tegen een aanval die probeert de kwetsbaarheid te exploiteren die in dit document wordt beschreven. De preventie van de bedreiging wordt bereikt door een standaardopheffing die een gebeurtenisactie voor teweeggebrachte handtekeningen met een *riskRatingValue* groter dan 90 uitvoert.

Voor aanvullende informatie over de risicorating en de berekening van de dreigingswaardering, de referentie Risicorating en de dreigingswaardering: Vereenvoudig IPS-beleidsbeheer.

Cisco-systeem voor beveiligingsbewaking, analyse en respons

Identificatie: incidenten van Cisco-systeem voor beveiligingsbewaking, analyse en respons

Het apparaat Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) kan incidenten veroorzaken met betrekking tot gebeurtenissen die verband houden met de kwetsbaarheid die in dit document wordt beschreven met behulp van IPS-handtekeningen 38247/0 (Handtekeningnaam: Cisco Content Services Gateway Denial of Service). Nadat de S580 dynamische handtekeningupdate is gedownload, zal het gebruik van sleutelwoord **NR-38247/0** voor IPS handtekening 38247/0 en een vraagtype van **Alle overeenkomende gebeurtenissen** op Cisco Security MARS applicatie een rapport leveren dat een lijst maakt van de incidenten die door de IPS handtekening zijn gemaakt.

Beginnend met de versies 4.3.1 en 5.3.1 van Cisco Security MARS-apparaten, is de ondersteuning voor de functie van Cisco IPS dynamische handtekeningen toegevoegd. Deze functie downloadt nieuwe handtekeningen van Cisco.com of van een lokale webserver, verwerkt en categoriseert correct ontvangen gebeurtenissen die overeenkomen met die handtekeningen, en omvat ze in inspectieregels en rapporten. Deze updates bieden normalisatie van gebeurtenissen en gebeurtenisgroepstoewijzing, en ze stellen ook het MARS-apparaat in staat om nieuwe handtekeningen van de IPS-apparaten te parseren.

Waarschuwing: als dynamische handtekeningupdates niet zijn geconfigureerd, worden gebeurtenissen die deze nieuwe handtekeningen weergeven als *onbekend gebeurtenistype* in vragen en rapporten. Omdat MARS deze gebeurtenissen niet opneemt in de inspectieregels, kunnen incidenten niet worden gecreëerd voor potentiële bedreigingen of aanvallen die binnen het netwerk plaatsvinden.

Deze optie is standaard ingeschakeld, maar moet geconfigureerd worden. Als deze niet is geconfigureerd, wordt de volgende Cisco Security MARS-regel geactiveerd:

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

Wanneer deze functie is ingeschakeld en geconfigureerd, kunnen beheerders de huidige versie van handtekeningen die door MARS is gedownload, bepalen door **Help > Info** te selecteren en de waarde voor *IPS Signature Version* te bekijken.

Er is aanvullende informatie over updates van dynamische handtekeningen en instructies voor het configureren van dynamische handtekeningupdates beschikbaar voor de releases van Cisco Security MARS 4.3.1 en 5.3.1.

Aanvullende informatie

Revisiegeschiedenis

Revisie 1.0	2011-juli-2006	Eerste openbare publicatie

Cisco-beveiligingsprocedures

Volledige informatie over het melden van beveiligingskwetsbaarheden in Cisco-producten, het verkrijgen van assistentie bij beveiligingsincidenten en het registreren om beveiligingsinformatie van Cisco te ontvangen, is beschikbaar op de wereldwijde website van Cisco op https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dit omvat instructies voor persvragen over Cisco-beveiligingsmeldingen. Alle Cisco-beveiligingsadviezen zijn beschikbaar op http://www.cisco.com/go/psirt.

Gerelateerde informatie

- Cisco-bulletins voor toegepaste beperking
- Cisco-beveiliging
- Cisco Security IntelliShield Alert Manager-service
- Cisco-handleiding over het versterken van Cisco IOS-apparaten
- Cisco IOS NetFlow - startpagina op Cisco.com
- Cisco IOS NetFlow-witboeken
- NetFlow-prestatieanalyse
- Witboeken voor Cisco Network Foundation-bescherming
- Presentaties voor Cisco Network Foundation-bescherming
- Een security georiënteerde benadering van IP-adressering
- Inzicht in bescherming van besturingsplane
- Opdrachttaal voor gereedschap beveiligen op Cisco IOS
- Cisco Firewallproducten - startpagina op Cisco.com
- Cisco-inbraakpreventiesysteem
- Cisco-downloads voor IPS-handtekeningen
- Cisco-zoekpagina voor IPS-handtekeningen
- Cisco-systeem voor beveiligingsbewaking, analyse en respons
- Gemeenschappelijke kwetsbaarheden en blootstellingen (CVE)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.