Het identificeren en beperken van exploitatie van de meervoudige kwaliteiten in de Cisco ACE-module voor Application Control Engine en Cisco ACE 4710 Application Control Engine

Advies-ID: Cisco CATALYST-2010/811-AXE switch

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100811-ace

Herziening 1.1

Voor de openbare release 2010, 11:16:00 UTC (GMT)

Inhoud

Cisco-respons

Dit Applied Mitigation Bulletin is een metro document naar de PSIRT Security Adviserende *Meervoudige kwaliteiten in de Cisco ACE-module van de Application Control Engine en Cisco ACE 4710 Application Control Engine* en biedt identificatie- en verzachtingstechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

Er zijn meerdere kwetsbaarheden in Cisco ACE-module voor Application Control Engine en Cisco ACE 4710 Application Control Engine. Deze subparagrafen vatten deze kwetsbaarheden samen:

Real-Time Streaming Protocol (RTSP), inspectie-ontkenning van de kwetsbaarheid voor services: Deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie van de eindgebruiker. Succesvolle exploitatie van deze kwetsbaarheid kan ervoor zorgen dat het getroffen apparaat kan crashen, wat kan leiden tot een 'denial of service'-toestand (DoS). Herhaalde pogingen om deze kwetsbaarheid uit te buiten zouden kunnen resulteren in een duurzame DoS-toestand. De aanvalsvector voor exploitatie is door RTSP-pakketten die TCP poort 554 gebruiken.

Deze kwetsbaarheid heeft CVE-identificator CVE-2010-2822 gekregen.

HTTP, RTSP en Session Initiation Protocol (SIP), inspectie-ontkenning van de kwetsbaarheid van

de service: Deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie van de eindgebruiker. Een geslaagde exploitatie van deze kwetsbaarheid kan ertoe leiden dat het aangetaste apparaat crasht, wat resulteert in een DOS-toestand. Herhaalde pogingen om deze kwetsbaarheid uit te buiten zouden kunnen resulteren in een duurzame DoS-toestand.

De aanval vectoren voor exploitatie zijn door pakketten die deze protocollen en poorten gebruiken:

- HTTP met TCP-poort 80
- RTSP met TCP-poort 554
- SIP met TCP-poort 5060

Deze kwetsbaarheid heeft CVE-identificator CVE-2010-2823 gekregen.

SSL Denial of Service Vulnerability: Deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie van de eindgebruiker. Een geslaagde exploitatie van deze kwetsbaarheid kan ertoe leiden dat het aangetaste apparaat crasht, wat resulteert in een DOS-toestand. Herhaalde pogingen om deze kwetsbaarheid uit te buiten zouden kunnen resulteren in een duurzame DoS-toestand. De aanval vector voor exploitatie is door SSL pakketten die TCP poort 443 gebruiken.

Deze kwetsbaarheid heeft CVE-identificator CVE-2010-2824 gekregen.

Kwetsbaarheid van SIP-inspectie en ontkenning van service: Deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie van de eindgebruiker. Een geslaagde exploitatie van deze kwetsbaarheid kan ertoe leiden dat het aangetaste apparaat crasht, wat resulteert in een DOS-toestand. Herhaalde pogingen om deze kwetsbaarheid uit te buiten zouden kunnen resulteren in een duurzame DoS-toestand.

De aanval vectoren voor exploitatie zijn door pakketten die deze protocollen en poorten gebruiken:

- SIP met TCP-poort 5060
- SIP met UDP-poort 5060

Een aanvaller zou deze kwetsbaarheden kunnen uitbuiten door spoofed pakketten te gebruiken.

Deze kwetsbaarheid heeft CVE-identificator CVE-2010-2825 gekregen.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory, die beschikbaar is op de volgende link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100811-ace.

Overzicht van beheertechnieken

Cisco-apparaten bieden verschillende tegenmaatregelen voor deze kwetsbaarheden. Administrateurs wordt aangeraden deze beveiligingsmethoden te beschouwen als algemene beveiligingsbeste praktijken voor infrastructuurvoorzieningen en het verkeer dat het netwerk overbrengt. Dit deel van het document geeft een overzicht van deze technieken.

Cisco IOS® Software kan effectieve manier van uitbuiting bieden met behulp van Infrastructuur Access Control List (iACL's). Dit beschermingsmechanisme filters en druppelt pakketten die deze kwetsbaarheden proberen uit te buiten.

Een effectieve preventie van misbruik kan ook worden geboden door Cisco ASA 5500 Series adaptieve security applicatie en de Firewallservicesmodule (FWSM) voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers met behulp van Transitotoegangscontrolelijsten (TACL's). Dit beschermingsmechanisme filters en druppelt pakketten die deze kwetsbaarheden proberen uit te buiten.

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

Cisco IOS NetFlow-records kunnen zichtbaarheid bieden in op netwerk gebaseerde pogingen tot exploitatie.

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

Het apparaat van Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) kan ook zichtbaarheid bieden door incidenten, vragen en rapportage van gebeurtenissen.

Risicobeheer

Organisaties wordt geadviseerd hun standaard risicobeoordelings- en risicobeperkingsprocessen te volgen om de mogelijke gevolgen van deze kwetsbaarheden te bepalen. Triage verwijst naar het sorteren van projecten en het prioriteren van inspanningen die waarschijnlijk een succes zullen worden. Cisco heeft documenten verstrekt die organisaties kunnen helpen een op risico gebaseerde triage mogelijkheid voor hun informatiebeveiligingsteams te ontwikkelen. Risk Triage voor Security Vulnerability aankondigingen en Risk Triage en Protocoltypering kunnen organisaties helpen om herhaalbare veiligheidsevaluatie en responsprocessen 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 configuratie wijziging, dient u het effect van deze configuratie te evalueren voordat u de wijziging toepast.

Voor deze hulpmiddelen is specifieke informatie over mitigatie 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

Beperken: Toegangscontrolelijsten voor infrastructuur

Om infrastructurele apparaten te beschermen en de risico's, impact en effectiviteit van directe infrastructuuraanvallen te minimaliseren, worden beheerders geadviseerd om iACL's in te zetten om beleidshandhaving van verkeer dat naar infrastructurele apparatuur wordt verzonden uit te voeren. De beheerders kunnen een iACL bouwen door uitdrukkelijk toe te staan enkel toegestaan

verkeer naar infrastructurele apparaten in overeenstemming met bestaand veiligheidsbeleid en -configuraties. Voor een maximale bescherming van infrastructuurelementen dienen iACL's te worden toegepast in de ingangsrichting op alle interfaces waarvoor een IP-adres is ingesteld. Een iACL-werkgebied kan geen volledige bescherming tegen deze kwetsbaarheden bieden wanneer de aanval van een vertrouwd bronadres afkomstig is.

Het iACL-beleid ontkent onbevoegde SSL-pakketten op TCP poort 443 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld is 192.168.60.0/24 de IP adresruimte die door de getroffen apparaten wordt gebruikt, en de host op 192.168.100.1 wordt beschouwd als een betrouwbare bron die toegang tot de getroffen apparaten vereist. Zorg ervoor dat u het vereiste verkeer voor routing en administratieve toegang toestaat voordat u al onbevoegd verkeer loost. Waar mogelijk moet de ruimte van het infrastructuuradres verschillen van de adresruimte die wordt gebruikt voor gebruikers- en dienstensegmenten. Deze adresseringsmethodologie zal helpen bij de bouw en inzet van iACL's.

Aanvullende informatie over iACL's is in Protect Your Core: Toegangscontrolelijsten voor bescherming van infrastructuur.

```
 ip access-list extended Infrastructure-ACL-Policy
 ! !-- Include explicit permit statements for trusted sources !-- that require access on the vulnerable port ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443 ! !-- The following vulnerability-specific access control entry !-- (ACE) can aid in identification of attacks ! deny tcp any 192.168.60.0 0.0.0.255 eq 443 ! !-- 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
```

Merk op dat het filteren met een interface toegangslijst de transmissie van ICMP onbereikbare berichten terug naar de bron van het gefilterde verkeer zal opleveren. Het genereren van deze berichten zou het ongewenste effect kunnen hebben van het verhogen van het CPU-gebruik op het apparaat. In Cisco IOS-software is de onbereikbare generatie van ICMP beperkt tot één pakket per 500 milliseconden standaard. ICMP onbereikbare berichtgeneratie kan worden uitgeschakeld met behulp van de opdracht voor de interfaceconconfiguratie **zonder ip onbereikbaar**. ICMP onbereikbare snelheidsbeperking kan van de standaard gewijzigd worden door de **ip-mp rate-limit onbereikbaar** *interval-in-ms* te gebruiken.

Identificatie: Toegangscontrolelijsten voor infrastructuur

Nadat de beheerder iACL op een interface toepast, zal de opdracht van de **show ip toegang-lijsten** het aantal SSL pakketten op TCP poort 443 identificeren die op interfaces zijn gefilterd waarop iACL wordt toegepast. De beheerders zouden gefilterde pakketten moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheden te exploiteren. Uitvoer van het voorbeeld voor **tonen ip toegang-lijsten infrastructuur-ACL-beleid**:

```
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 443
    20 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (3713 matches)
    30 deny ip any 192.168.60.0 0.0.0.255
router#
```

In het bovenstaande voorbeeld, is de toegangslijst *Infrastructuur-ACL-beleid* gedaald **3713 SSL** pakketten op **TCP** poort **443 (https)** voor toegangscontrolelijst ingang (ACE) lijn 20.

Voor extra informatie over het onderzoeken van incidenten die ACE tellers en sysloggebeurtenissen gebruiken, verwees naar het Identificatie Incidenten die Firewall en IOS de Beelden van de toegepaste Intelligentie gebruiken.

De beheerders kunnen Cisco Embedded Event Manager gebruiken om instrumentatie te bieden wanneer aan specifieke voorwaarden wordt voldaan, zoals ACE teller hits. Het Applied Intelligence Witboek Embedded Event Manager in een beveiligingscontext geeft aanvullende informatie over hoe deze optie te gebruiken.

Identificatie: Vastlegging toegangslijst

De optie toegangscontrolelijst voor logbestanden en **logingingingangen** (ACL's) zorgt ervoor dat pakketten die overeenkomen met specifieke ACE's worden geregistreerd. De optie **log-invoer** maakt het registreren van de ingangsinterface mogelijk, naast de pakketbron en de IP-adressen en -poorten.

Voorzichtig: De loggen van de toegangscontrolelijst kunnen zeer CPU-intensief zijn en moeten met uiterste voorzichtigheid worden gebruikt. Factoren die het effect van de CPU van het registreren van ACL drijven zijn loggeneratie, logtransmissie en procesoverschakeling naar voorwaartse pakketten die log-enabled ACE's overeenkomen.

Voor Cisco IOS-software kan het **ip access-list loginterval** *interval-in-ms* opdracht de effecten van processwitching beperken die veroorzaakt worden door ACL logging. De *houtkap*-limiet *per seconde* [**behalve** *logniveau*] beperkt de impact van loggeneratie en transmissie.

Het CPU-effect van ACL-vastlegging kan in hardware worden aangepakt via Cisco Catalyst 6500 Series-switches en Cisco 7600 Series routers met Supervisor Engine 720 of Supervisor Engine 32 met gebruik van geoptimaliseerde ACL-loggen.

Raadpleeg voor meer informatie over de configuratie en het gebruik van ACL-vastlegging het witboek Begrijpingscontrolelijst voor toegangscontrole.

Cisco IOS NetFlow

Identificatie: Traffic Flow-identificatie met NetFlow-records

De beheerders kunnen Cisco IOS NetFlow op Cisco IOS routers en switches configureren om te helpen bij de identificatie van verkeersstromen die pogingen kunnen zijn om deze kwetsbaarheden te exploiteren. Beheerders wordt geadviseerd om stromen te onderzoeken om te bepalen of ze pogingen zijn om deze kwetsbaarheden uit te buiten of dat ze legitieme 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         192.168.10.203  Gi0/1         192.168.60.103  06 0986 01BB    37
Gi0/0         192.168.11.56   Gi0/1         192.168.60.178  06 0911 01BB    13
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    11 0016 01BB     1
Gi0/0         192.168.23.97   Gi0/1         192.168.60.18   06 0B3E 01BB     5
Gi0/0         192.168.12.12   Gi0/1         192.168.60.91   06 0B89 01BB     3
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  06 0BD7 01BB    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 **SSL** op **TCP** poort **443 (hex waarde 01BB)**.

Om alleen de verkeersstromen voor SSL-pakketten op TCP-poort 443 (hex-waarde 01B) te bekijken, **toont** de opdracht **ip cache-flow | Inclusief SrcAs|_06_.*01BB** toont de verwante TCP NetFlow records zoals hier wordt getoond:

```
router#show ip cache flow | include SrcIf|_06_.*01BB
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.203  Gi0/1         192.168.60.103  06 0986 01BB    37
Gi0/0         192.168.11.56   Gi0/1         192.168.60.178  06 0911 01BB    13
Gi0/0         192.168.23.97   Gi0/1         192.168.60.18   06 0B3E 01BB     5
Gi0/0         192.168.12.12   Gi0/1         192.168.60.91   06 0B89 01BB     3
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  06 0BD7 01BB    11
router#
```

Cisco ASA en FWSM firewalls

Beperken: Toegangscontrolelijsten voor douanevervoer

Om het netwerk te beschermen tegen verkeer dat het netwerk op ingangstoegangspunten ingaat, dat ook internetverbindingspunten, partner- en leverancierverbindingspunten of VPN-

verbindingspunten kan omvatten, worden de beheerders geadviseerd om ACL's in te voeren om beleid te handhaven. De beheerders kunnen een tACL bouwen door expliciet alleen toegestaan verkeer toe te staan om het netwerk te betreden bij ingangstoegangspunten of door geautoriseerd verkeer toe te staan om het netwerk door te voeren in overeenstemming met bestaand beveiligingsbeleid en -configuraties. Een TACL-werkgebied kan geen volledige bescherming tegen deze kwetsbaarheden bieden wanneer de aanval van een vertrouwd bronadres afkomstig is.

Het beleid tACL ontkent onbevoegde SSL pakketten op TCP poort 443 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld is 192.168.60.0/24 de IP adresruimte die door de getroffen apparaten wordt gebruikt, en de host op 192.168.100.1 wordt beschouwd als een betrouwbare bron die toegang tot de getroffen apparaten vereist. Zorg ervoor dat u het vereiste verkeer voor routing en administratieve toegang toestaat voordat u al onbevoegd verkeer loost.

Aanvullende informatie over tACL's bevindt zich in [toegangscontrolelijsten voor douanevervoer: Filtering aan uw rand](#).

```
! !-- Include explicit permit statements for trusted sources !-- that require access on the
vulnerable port ! access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 443 ! !-- The following vulnerability-specific access control entry !-- (ACE)
can aid in identification of attacks ! access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 443 ! !-- 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 op een interface is toegepast, kunnen de beheerders de opdracht **showaccess-list** gebruiken om het aantal SSL pakketten op TCP poort 443 te identificeren die zijn gefilterd. De beheerders worden geadviseerd om gefilterde pakketten te onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheden te exploiteren. Uitvoer van het voorbeeld voor **tonen toegang-lijst tACL-beleid**:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 3 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq https (hitcnt=3713)
access-list tACL-Policy line 2 extended deny tcp any
     192.168.60.0 255.255.255.0 eq https (hitcnt=221)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

In het bovenstaande voorbeeld, is de toegangslijst *tACL-beleid* gedaald **221 SSL** pakketten op **TCP** poort **443 (https)** ontvangen van een onvertrouwde host of netwerk. Bovendien kan syslogbericht *106023* waardevolle informatie bieden, die het bron- en bestemming IP-adres, de bron- en doelpoortnummers en het IP-protocol voor het ontkende pakket bevat.

Identificatie: Waarschuwingen voor firewalltoegangslijst

Firewallsyslogbericht *106023* zal worden gegenereerd voor pakketten die door een toegangscontrole ingang (ACE) worden ontkend die het **logsleutelwoord** niet aanwezig heeft. Aanvullende informatie over dit syslogbericht staat in [Cisco ASA 5500 Series System Log](#)

Message, 8.2-106023.

Informatie over het configureren van syslg voor Cisco ASA 5500 Series adaptieve security applicatie is in bewaking - configuratie van vastlegging. Informatie over het configureren van syslogon op FWSM voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers is bezig met bewaking van de firewallservicesmodule.

In het volgende voorbeeld, de **show logging logging | grep** *regex* commando haalt syslog berichten uit de houtkapbuffer op de firewall. Deze berichten bieden extra informatie over ontkende pakketten die op mogelijke pogingen kunnen wijzen om de kwetsbaarheden te exploiteren die in dit document worden beschreven. Het is mogelijk om verschillende reguliere expressies met het **grep** sleutelwoord te gebruiken om naar specifieke gegevens in de geregistreerde berichten te zoeken.

Aanvullende informatie over de syntaxis van reguliere expressies is in het maken van een reguliere expressie.

```
firewall#show logging | grep 106023
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
         dst inside:192.168.60.240/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
         dst inside:192.168.60.115/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
         dst inside:192.168.60.38/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.175/2950
         dst inside:192.168.60.250/443 by access-group "tACL-Policy"
firewall#
```

In het bovenstaande voorbeeld, de berichten die voor de tACL *tACL-beleid* zijn vastgelegd tonen **SSL**-pakketten voor **TCP** poort **443 (https)** die naar het adresblok zijn verzonden dat aan de getroffen apparaten is toegewezen.

Aanvullende informatie over syslig-berichten voor ASA security apparaten is in Cisco ASA 5500 Series System Log Messages, 8.2. Aanvullende informatie over syslogberichten voor ASA is te vinden in Catalyst 6500 Series switch en Cisco 7600 Series routermodule met firewall-logberichten.

Raadpleeg het witboek Identificatie van incidenten die incidenten met behulp van firewall en IOS Router Sising-gebeurtenissen onderzoeken die systeemgebeurtenissen gebruiken.

Cisco-inbraakpreventiesysteem

Beperken: Cisco IPS-handtekeningen

De beheerders kunnen Cisco IPS apparaten en servicesmodules gebruiken om bedreigingsdetectie te bieden en pogingen te voorkomen om de kwetsbaarheden te exploiteren die in dit document worden beschreven. Deze zwakheden kunnen door deze handtekeningen worden gedetecteerd:

- 27359/0 - Kwetsbaarheid voor RTSP-inspectie

- 2759/2009 - Cisco ACE-inspectie DOM-S

2739/00 - Kwetsbaarheid voor realtime streaming protocol voor inspectie

Beginnend met signatuur update S507 voor sensoren die Cisco IPS versie 6.x en meer draaien, kan deze kwetsbaarheid worden gedetecteerd door signatuur 27359/0 (Handelsnaam: Realtime streaming protocol inspectie (kwetsbaarheid). Signature 27359/0 wordt door default ingeschakeld, veroorzaakt een *High* Severity event, heeft een signatuur fidelity rating (SFR) van 90 en is ingesteld met een default event-actie van **producwaakzaamheid**.

Handtekening 27359/0 branden wanneer een specifieke poging om de kwetsbaarheid te exploiteren zoals gedocumenteerd door Cisco-identificator CSCta85227 wordt gedetecteerd. Het afvuren van deze handtekening kan wijzen op een potentieel misbruik van deze kwetsbaarheid.

2759/2009 - Cisco ACE-inspectie DOM-S

Beginnend met signatuur update S507 voor sensoren die Cisco IPS versie 6.x en meer draaien, kan deze kwetsbaarheid worden gedetecteerd door signatuur 27599/0 (Handelsnaam: Cisco ACE SIP-inspectie (DOS). Signature 27599/0 wordt door default ingeschakeld, veroorzaakt een *Medium* Severity event, heeft een signatuur-fidelity rating (SFR) van 85, en is ingesteld met een standaardoffactie van **producwaakzaamheid**.

Handtekening 27599/0 branden wanneer een specifieke poging wordt gedetecteerd om de kwetsbaarheden te exploiteren die zijn gedocumenteerd door Cisco-identificatoren CSCta65603 en CSCta71569. Het afvuren van deze handtekening kan wijzen op een potentieel misbruik van deze kwetsbaarheid.

De beheerders kunnen Cisco IPS sensoren configureren om een gebeurtenis actie uit te voeren wanneer een aanval wordt gedetecteerd. De geconfigureerde event-actie voert preventieve of afschrikkende controles uit om te helpen beschermen tegen een aanval die probeert de kwetsbaarheden te exploiteren die in dit document worden beschreven.

Explosies die gespoofde IP-adressen gebruiken kunnen een geconfigureerde eventactie veroorzaken om onbedoeld verkeer van vertrouwde bronnen te ontkennen.

Cisco IPS-sensoren zijn het effectiefst bij gebruik in inline security modus in combinatie met het gebruik van een eventactie. Automatische bedreigingspreventie voor Cisco IPS 6.x en grotere sensoren die in inline security modus worden ingezet, bieden bedreigingspreventie tegen een aanval die probeert de kwetsbaarheden te exploiteren die in dit document worden beschreven. Threat Prevention wordt bereikt door een defaultwachtwoord dat een gebeurtenis actie uitvoert voor geactiveerd handtekeningen met een *riskRatingValue* groter dan 90.

Voor aanvullende informatie over de berekening van de risicoclassificatie en de dreigingsrating, de referentie-risicoratings en de risicoratings: Vereenvoudig IPS-beleidsbeheer.

Cisco-systeem voor beveiligingsbewaking, -analyse en -respons

Identificatie: Incidenten van Cisco Security Monitoring, Analysis en Response System

Het apparaat van Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) kan incidenten creëren met betrekking tot gebeurtenissen die betrekking hebben op de kwetsbaarheden die in dit document worden beschreven met IPS-handtekeningen 27359/0

(Handelsnaam: Real-time Streaming Protocol inspection kwetsbaarheid) en 27599/0 (Handelsnaam: Cisco ACE SIP-inspectie (DOS). Nadat het dynamische signatuur van S507 is gedownload, gebruikmakend van sleutelwoord **NR-27359/0** voor IPS signatuur 27359/0 of **NR-27599/0** voor IPS signatuur 27599/0 en een vraagtype van **All Matching Event Reling Event Berichten** Op het Cisco Security MARS-apparaat wordt een rapport geleverd dat een lijst maakt van de incidenten die door de IPS-handtekening zijn gemaakt.

Beginnend met de releases van Cisco Security MARS-apparatuur van 4.3.1 en 5.3.1 is ondersteuning voor de functie voor dynamische handtekeningen van Cisco IPS toegevoegd. Deze optie downloads nieuwe handtekeningen van Cisco.com of van een lokale webserver, verwerkt en categoriseert ontvangen gebeurtenissen die overeenkomen met deze handtekeningen en bevat deze in inspectieregels en rapporten. Deze updates verstrekken gebeurtenis normalisatie en gebeurtenis groepstoewijzing, en zij stellen ook het apparaat van MARS in staat om nieuwe handtekeningen van de IPS apparaten te ontleden.

Voorzichtig: Als dynamische signatuur updates niet worden gevormd, verschijnen gebeurtenissen die deze nieuwe handtekeningen aan elkaar koppelen als *onbekend* voorval type in vragen en rapporten. Omdat MARS deze gebeurtenissen niet in inspectieregels zal opnemen, kunnen er geen incidenten worden gecreëerd tegen mogelijke bedreigingen of aanvallen die binnen het netwerk plaatsvinden.

Deze optie is standaard ingeschakeld maar moet zijn geconfigureren. Als deze niet is ingesteld, wordt deze Cisco Security MARS-regel geactiveerd:

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

Wanneer deze optie ingeschakeld en geconfigureerd is, kunnen beheerders de huidige versie van de handtekening die door MARS is gedownload, bepalen door **Help > About** te selecteren en de waarde van de *IPS-handtekeningen te* herkennen.

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

Aanvullende informatie

DIT DOCUMENT WORDT AANGEBODEN OP EEN ‘AS IS’-BASIS EN IMPLICEERT GEEN ENKEL SOORT GARANTIE, MET INBEGRIP VAN GARANTIES VAN VERKOOPBAARHEID OF GESCHIKTHEID VOOR EEN BEPAALD DOEL. UW GEBRUIK VAN DE INFORMATIE IN HET DOCUMENT OF DE MATERIALEN GEKOPPELD AAN HET DOCUMENT IS GEHEEL OP EIGEN RISICO. CISCO BEHOUDT ZICH HET RECHT VOOR OM DIT DOCUMENT TE ALLEN TIJDE TE WIJZIGEN OF TE ANNULEREN.

Historie herziening

Herziening 1.1	2010-11 augustus	Verwijzingen naar IPS-handtekeningen 28301/0 verwijderen.
Herziening 1.0	2010-11 augustus	Eerste publieke vrijlating.

Cisco-beveiligingsprocedures

Volledige informatie over het rapporteren van security kwetsbaarheden in Cisco-producten, het verkrijgen van hulp met veiligheidsincidenten en het registreren om veiligheidsinformatie van Cisco te ontvangen, is beschikbaar op de website van Cisco wereldwijd op http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. Dit omvat instructies voor persvragen betreffende Cisco veiligheidsmededelingen. Alle Cisco-beveiligingsadviezen zijn beschikbaar op http://www.cisco.com/go/psirt.

Gerelateerde informatie

- Cisco toegepaste limiteringsbulletins
- Cisco-beveiligingsinformatieoperaties
- Cisco Security IntelliShield Alert Manager-service
- Cisco IOS NetFlow - startpagina op Cisco.com
- Cisco IOS NetFlow-witboeken
- NetFlow-prestatieanalyse
- Cisco Firewallproducten - startpagina op Cisco.com
- Cisco-inbraakpreventiesysteem
- Cisco IPS-handdownloads
- Zoekpagina voor Cisco IPS-handtekeningen
- Cisco-systeem voor beveiligingsbewaking, -analyse en -respons
- Vaak voorkomende zwakheden en blootstellingen (CVE)