Identificatie en beperking van exploitatie van de kwetsbaarheid voor Cisco IOS-software en IP-serviceniveau

Identificatie en beperking van exploitatie van de kwetsbaarheid voor Cisco IOS-software en IP-serviceniveau

Advies-ID: cisco-amb-20110928-ipsla

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110928-ipsla

Revisie 1.1

Voor Openbare Publicatie 2011 September 28 16:00 UTC (GMT)

Inhoud

Cisco Response

Dit Toegepaste Matiging Bulletin is een begeleidend document bij de PSIRT Security Advisory *Cisco IOS-software en* de *kwetsbaarheid voor IP*-serviceniveau-*overeenkomst* en biedt identificatie- en mitigatietechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

De functie Cisco IOS-softwarerelease IP-serviceniveau (IP SLA) bevat een kwetsbaarheid wanneer deze speciaal vervaardigde IP SLA-pakketten verwerkt. Deze kwetsbaarheid kan op afstand worden benut zonder authenticatie en zonder interactie van de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan het betreffende apparaat vastlopen. Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie. De aanvalsvector voor exploitatie is via IP SLA-pakketten met UDP-poort 1967 en andere geconfigureerde en dynamisch toegewezen UDP-poorten. Een aanvaller kon deze

kwetsbaarheid exploiteren met spoofed pakketten.

Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-3272.

Overzicht van kwetsbaarheden

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-20110928-ipsla.

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 de volgende methoden:

- Toegangscontrolelijsten voor infrastructuur (iACL's)
- Unicast Reverse Path Forwarding (Unicast RPF)
- IP-bronbeveiliging (IPSG)

Deze beschermingsmechanismen filteren en laten vallen, en verifiëren het IP-adres van de bron van pakketten die deze kwetsbaarheid proberen te exploiteren.

De juiste implementatie en configuratie van Unicast RPF biedt een effectieve bescherming tegen aanvallen die pakketten met IP-adressen van gespoofde bronnen gebruiken. Unicast RPF moet zo dicht mogelijk bij alle verkeersbronnen worden geïmplementeerd.

De juiste plaatsing en configuratie van IPSG biedt een effectief middel tegen spoofingaanvallen op de toegangslaag.

Er kunnen ook effectieve middelen voor explosiepreventie worden geleverd door de Cisco ASA 5500 Series adaptieve security applicatie en de Firewall Services Module (FWSM) voor Cisco Catalyst 6500 Series switches die de volgende methoden gebruiken:

- Toegangscontrolelijsten voor douanevervoer (ACL's)
- Unicast RPF

Deze beschermingsmechanismen filteren en laten vallen, en verifiëren het IP-adres van de bron van pakketten die deze kwetsbaarheid proberen te exploiteren.

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

Cisco IOS-software, Cisco ASA, Cisco FWSM-firewalls en Cisco ACE Application Control Engine-applicatie en -module kunnen zichtbaarheid bieden door middel van syslogberichten en tegenwaarden die in de uitvoer van **show-**opdrachten worden weergegeven.

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 IOS-routers en -Switches

Beperking: toegangscontrolelijsten voor infrastructuur

Om infrastructuurapparaten te beschermen en het risico, de impact en de effectiviteit van directe infrastructuuraanvallen te minimaliseren, wordt beheerders aangeraden om lijsten met toegangscontroles voor de infrastructuur (iACL's) te implementeren om beleidshandhaving uit te voeren van verkeer dat naar infrastructuurapparatuur wordt verzonden. Beheerders kunnen een iACL construeren door alleen geautoriseerd verkeer toe te staan dat naar infrastructuurapparaten wordt verzonden in overeenstemming met bestaand beveiligingsbeleid en configuraties. Voor een maximale bescherming van infrastructurele apparaten moeten gebruikte iACL's worden toegepast in de toegangsrichting op alle interfaces waarvoor een IP-adres is geconfigureerd. Een iACL-tijdelijke oplossing kan geen volledige bescherming tegen deze kwetsbaarheid bieden wanneer de aanval afkomstig is van een vertrouwd bronadres.

Het iACL-beleid ontkent onbevoegde IP SLA-pakketten op UDP-poort 1967 die naar getroffen apparaten worden verzonden. Opgemerkt moet worden dat het blokkeren van de toegang tot UDP-poort 1967 apparaten niet volledig beschermt. Als Cisco IOS IP SLA is geconfigureerd met permanente poorten, moeten deze geconfigureerde poorten ook aan de iACL worden toegevoegd. 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. Waar mogelijk moet de adresruimte van de infrastructuur worden onderscheiden van de adresruimte die wordt gebruikt voor gebruikers- en dienstensegmenten. Het gebruik van deze adresseringsmethodologie zal helpen bij de constructie en implementatie van iACL's.

Aanvullende informatie over iACL's is te vinden in Protected Your Core: Infrastructure Protection Access Control Lists.

```
 ip access-list extended Infrastructure-ACL-Policy


!
!-- Include explicit permit statements for trusted sources
!-- that require access on the vulnerable port
!
 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1967
!
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
!
 deny udp any 192.168.60.0 0.0.0.255 eq 1967
!
!-- 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 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*.

Beperken: bescherming tegen spoofing

Unicast doorsturen van omgekeerde paden

De kwetsbaarheid die in dit document wordt beschreven, kan worden benut door gespoofde IP-pakketten. Beheerders kunnen Unicast Reverse Path Forwarding (Unicast RPF) implementeren en configureren als een beschermingsmechanisme tegen spoofing.

Unicast RPF is geconfigureerd op interfaceniveau en kan pakketten detecteren en neerzetten die geen verifieerbaar IP-bronadres hebben. Beheerders dienen niet te vertrouwen op Unicast RPF om volledige bescherming tegen spoofing te bieden, omdat spoofed-pakketten het netwerk via een Unicast RPF-enabled interface kunnen binnenkomen als er een geschikte retourroute naar het bron-IP-adres bestaat. Beheerders wordt aangeraden ervoor te zorgen dat de juiste Unicast RPF-modus (los of strikt) wordt geconfigureerd tijdens de implementatie van deze functie, omdat legitiem verkeer dat het netwerk oversteekt kan worden geminimaliseerd. In een ondernemingsmilieu, zou Unicast RPF bij de rand van Internet en de interne toegangslaag op gebruiker-ondersteunende Layer 3 kunnen worden toegelaten interfaces.

Aanvullende informatie vindt u in de Unicast Reverse Path Forwarding Losse Mode functiehandleiding.

Voor extra informatie over de configuratie en het gebruik van Unicast RPF, verwijs naar het

Witboek Understanding Unicast Reverse Path Forwarding Applied Intelligence.

IP-bronbeveiliging

IP Source Guard (IPSG) is een beveiligingsfunctie die IP-verkeer op niet-gerouteerde, Layer 2-interfaces beperkt door pakketten te filteren op basis van de bindende database met DHCP-snooping en handmatig ingestelde IP-bronbindingen. Beheerders kunnen IPSG gebruiken om aanvallen te voorkomen van een aanvaller die probeert pakketten te parasiteren door het IP-bronadres en/of het MAC-adres te vervalsen. Wanneer correct geïmplementeerd en geconfigureerd, biedt IPSG in combinatie met de strikte modus Unicast RPF de meest effectieve bescherming tegen spoofing voor de kwetsbaarheid die in dit document wordt beschreven.

Aanvullende informatie over de implementatie en configuratie van IPSG is te vinden in Configureren DHCP-functies en IP Source Guard.

Identificatie: Toegangscontrolelijsten voor infrastructuur

Nadat de beheerder iACL op een interface toepast, zal de **opdracht IP-toegangslijsten tonen** het aantal IP SLA-pakketten op UDP-poort 1967 identificeren die zijn gefilterd op interfaces waarop iACL wordt toegepast. De beheerders zouden gefilterde pakketten moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont ip toegang-lijsten Infrastructuur-ACL-Beleid** volgt:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1967
    20 deny udp any 192.168.60.0 0.0.0.255 eq 1967 (49 matches)
    30 deny ip any 192.168.60.0 0.0.0.255
router#
```

In het vorige voorbeeld is *de* toegangslijst *Infrastructuur-ACL-Beleid* gedaald met **49 IP SLA-**pakketten op **UDP-poort 1967** voor regel 20 van de toegangscontrolelijst (ACE).

Voor extra informatie over het onderzoeken van incidenten met ACE-tellers en syslog-gebeurtenissen, raadpleegt u de 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.

Identificatie: bescherming tegen spoofing met Unicast Reverse Path Forwarding

Met Unicast RPF correct geïmplementeerd en geconfigureerd in de netwerkinfrastructuur, kunnen beheerders de *sleuf/poort* van het *type* show cef *interfacetype intern* gebruiken, **ip-interface tonen**, **cef-drop tonen**, **ip cef-switching statistieken-functie tonen**, en **ip traffic** opdrachten tonen om het aantal pakketten te identificeren dat Unicast RPF is gedaald.

Opmerking: beginnend met Cisco IOS-softwarerelease 12.4(20)T is de opdracht **ip cef-switching** vervangen door de **functie** IP **cef-switching**.

Opmerking: de *opdracht* **show | begin met** *regex* en **toon** *opdracht* **|** *regex*-opdrachtwijzigingen **omvatten** die in de volgende voorbeelden worden gebruikt om de hoeveelheid output te minimaliseren die beheerders moeten parseren om de gewenste informatie te bekijken. Er is aanvullende informatie over opdrachtbepalingen in de secties van de opdracht show van de opdrachtreferentie voor Cisco IOS Configuration Fundamentals.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop

  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0
router#
```

Opmerking: tonen cef interface *type sleuf / poort* **intern** is een verborgen opdracht die volledig moet worden ingevoerd op de opdrachtregel interface. Opdrachtvoltooiing is er niet voor beschikbaar.

```
router#show ip interface GigabitEthernet 0/0 | begin verify

  IP verify source reachable-via RX, allow default, allow self-ping
  18 verification drops
  0 suppressed verification drops
router#
```

```
router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route      No_adj  ChkSum_Err
RP            27           0           0          18           0           0
router#

router#show ip cef switching statistics feature

IPv4 CEF input features:
Path   Feature               Drop    Consume       Punt  Punt2Host Gave route
```

```
RP PAS uRPF                      18          0          0          0          0
Total                            18          0          0          0          0
    --      CLI Output Truncated       --
router#


router#show ip traffic | include RPF
         18 no route, 18 unicast RPF, 0 forced drop
router#
```

In de bovenstaande **show cef drop**, **toon ip cef switching statistieken functie**, en **toon ip traffic** voorbeelden, Unicast RPF heeft laten vallen **18 IP SLA pakketten** die globaal ontvangen op alle interfaces met Unicast RPF geconfigureerd vanwege het onvermogen om het bronadres van de IP pakketten te verifiëren binnen de Forwarding Information Base van Cisco Express Forwarding.

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 11 0984 07AF 1
Gi0/0 192.168.11.54 Gi0/1 192.168.60.158 11 0911 07AF 3
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 11 0B3E 07AF 5
Gi0/0 192.168.10.17 Gi0/1 192.168.60.97 11 0B89 07AF 1
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  06 007B 007B     1
Gi0/0 192.168.12.185 Gi0/1 192.168.60.239 11 0BD7 07AF 1
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
router#
```

In het vorige voorbeeld zijn er meerdere stromen voor **IP SLA** op **UDP** poort **1967 (hex-waarde 07AF)**.

Dit verkeer wordt afkomstig van en verzonden naar adressen binnen het 192.168.60.0/24 adresblok, dat voor infrastructuurapparaten wordt gebruikt. De pakketten in deze stromen kunnen worden gespoofd en kunnen wijzen op een poging om deze kwetsbaarheid te exploiteren. De beheerders worden geadviseerd om deze stromen bij basislijngebruik voor IP SLA verkeer te vergelijken dat op UDP haven 1967 wordt verzonden en ook de stromen te onderzoeken om te bepalen of zij van onbetrouwbare gastheren of netwerken afkomstig zijn.

Als u alleen de verkeersstromen voor IP SLA-pakketten op UDP-poort 1967 wilt weergeven (hex-waarde 07AF), **toont** de opdracht **ip-cachestroom | neem SrcIf|_11_.*07AF** zal de verwante verslagen van UDP NetFlow zoals hier getoond tonen:

UDP-stromen

```
router#show ip cache flow | include SrcIf|_11_.*07AF
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0 192.168.10.201 Gi0/1 192.168.60.102 11 0984 07AF 1
Gi0/0 192.168.11.54 Gi0/1 192.168.60.158 11 0911 07AF 3
Gi0/0 192.168.13.97 Gi0/1 192.168.60.28 11 0B3E 07AF 5
Gi0/0 192.168.10.17 Gi0/1 192.168.60.97 11 0B89 07AF 1
Gi0/0 192.168.12.185 Gi0/1 192.168.60.239 11 0BD7 07AF 1
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 IP SLA-pakketten op UDP-poort 1967 die naar getroffen apparaten worden verzonden. Opgemerkt moet worden dat het blokkeren van de toegang tot UDP-poort 1967 apparaten niet volledig beschermt. Als IP SLA is geconfigureerd met permanente poorten, moeten deze geconfigureerde poorten ook aan de iACL worden toegevoegd. 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 de Transit Access Control Lists: Filtering at Your Edge .

```
!
!-- Include explicit permit statements for trusted sources
!-- that require access on the vulnerable port
!
 access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 1967
!
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
!
 access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 1967

!
!-- 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
```

Beperking: bescherming tegen spoofing met Unicast Reverse Path Forwarding

De kwetsbaarheid die in dit document wordt beschreven, kan worden benut door gespoofde IP-pakketten. Beheerders kunnen Unicast RPF implementeren en configureren als een beschermingsmechanisme tegen spoofing.

Unicast RPF is geconfigureerd op interfaceniveau en kan pakketten detecteren en neerzetten die geen verifieerbaar IP-bronadres hebben. Beheerders dienen niet te vertrouwen op Unicast RPF om volledige bescherming tegen spoofing te bieden, omdat spoofed-pakketten het netwerk via een Unicast RPF-enabled interface kunnen binnenkomen als er een geschikte retourroute naar het bron-IP-adres bestaat. In een ondernemingsmilieu, zou Unicast RPF bij de rand van Internet en bij de interne toegangslaag op gebruiker-ondersteunende Layer 3 kunnen worden toegelaten interfaces.

Voor extra informatie over de configuratie en het gebruik van Unicast RPF, raadpleegt u de opdrachtreferentie van Cisco Security Appliance voor IP-verificatie van het omgekeerde pad en het witboek Understanding Unicast Reverse Path Forwarding Applied Intelligence.

Identificatie: Toegangscontrolelijsten voor douanevervoer

Nadat tACL is toegepast op een interface, kunnen beheerders de **show access-list** opdracht gebruiken om het aantal IP SLA-pakketten op UDP-poort 1967 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; 3 elements
access-list tACL-Policy line 1 extended permit udp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 1967
access-list tACL-Policy line 2 extended deny udp any
     192.168.60.0 255.255.255.0 eq 1967 (hitcnt=91)
access-list tACL-Policy line 3 extended deny ip any any
firewall#
```

In het vorige voorbeeld is de toegangslijst *van ACL-Policy* **91 IP SLA-**pakketten gedaald op **UDP-poort 1967** voor ACE-lijn 2.

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 Een reguliere expressie maken.

```
firewall#show logging | grep 106023
  Sep 28 2011 00:11:08: %ASA-4-106023: Deny udp src outside:192.0.2.18/5934
         dst inside:192.168.60.191/1967 by access-group "tACL-Policy"
  Sep 28 2011 00:11:08: %ASA-4-106023: Deny udp src outside:192.0.2.200/5935
         dst inside:192.168.60.33/1967 by access-group "tACL-Policy"
  Sep 28 2011 00:11:08: %ASA-4-106023: Deny udp src outside:192.0.2.99/5936
         dst inside:192.168.60.240/1967 by access-group "tACL-Policy"
  Sep 28 2011 00:11:08: %ASA-4-106023: Deny udp src outside:192.0.2.100/5937
         dst inside:192.168.60.115/1967 by access-group "tACL-Policy"
  Sep 28 2011 00:11:08: %ASA-4-106023: Deny udp src outside:192.0.2.88/5938
         dst inside:192.168.60.38/1967 by access-group "tACL-Policy"
  Sep 28 2011 00:11:08: %ASA-4-106023: Deny udp src outside:192.0.2.175/5939
         dst inside:192.168.60.250/1967 by access-group "tACL-Policy"
firewall#
```

In het vorige voorbeeld, tonen de berichten die voor tACL *tACL-Policy* worden geregistreerd potentieel gespoofde **IP SLA-**pakketten voor **UDP-poort 1967** die naar het adresblok worden gestuurd dat aan de infrastructuurapparaten is 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 Use Firewall en IOS Router Syslog Events Applied Intelligence.

Identificatie: bescherming tegen spoofing met Unicast Reverse Path Forwarding

Firewallsyslog-bericht *106021* wordt gegenereerd voor pakketten die worden geweigerd door Unicast PDF. Aanvullende informatie over dit syslogbericht wordt weergegeven in Cisco ASA 5500 Series systeemlogbericht, 8.2 - 106021.

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 Een reguliere expressie maken.

```
firewall#show logging | grep 106021
  Sep 28 2011 00:11:08: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Sep 28 2011 00:11:08: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Sep 28 2011 00:11:08: %ASA-1-106021: Deny TCP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
```

De opdracht **Snel** starten tonen kan ook het aantal pakketten identificeren dat de Unicast RPF-functie is gevallen, zoals in het volgende voorbeeld:

```
firewall#show asp drop frame rpf-violated
  Reverse-path verify failed                      11
firewall#
```

In het voorafgaande voorbeeld heeft Unicast RPF **11 IP SLA-pakketten** laten vallen die zijn ontvangen op interfaces met Unicast RPF geconfigureerd. Het ontbreken van uitvoer geeft aan dat de Unicast RPF-functie op de firewall geen pakketten heeft laten vallen.

Voor extra informatie over het debuggen van versnelde security pad gedropte pakketten of verbindingen, raadpleeg de Cisco Security Appliance Command Reference voor show asp drop.

Aanvullende informatie

Revisiegeschiedenis

Revisie 1.0	2011-28 SEPTEMBER	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-beveiligingsintelligentie
- 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
- Identificatie en beperking van TTL-aanval bij verlopen
- 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
- Verbeteringen in Unicast Reverse Path Forwarding voor de Internet Service Provider
- 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.