Meervoudige kwetsbaarheden in Cisco TelePresence-producten identificeren en beperken

Meervoudige kwetsbaarheden in Cisco TelePresence-producten identificeren en beperken

Advies-ID: cisco-amb-20110223-telepresence

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110223-telepresence

Revisie 1.1

2011 februari 23 16:00 UTC (GMT)

Inhoud

Cisco Response

Dit Toegepaste Mitigation Bulletin is een begeleidend document bij de PSIRT Cisco TelePresence Bundle van Security Advisories en biedt identificatie- en onderdrukkingstechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren. De individuele veiligheidsadviseurs die onder deze AMB vallen, zijn als volgt:

- Meervoudige kwetsbaarheden in Cisco TelePresence-endpointapparaten
- Meervoudige kwetsbaarheden in Cisco TelePresence Manager
- Meervoudige kwetsbaarheden in Cisco TelePresence Multipoint Switch
- Meervoudige kwetsbaarheden in Cisco TelePresence Recording Server

Kwetsbaarheid Kenmerken

Er zijn meerdere kwetsbaarheden in Cisco TelePresence-producten. In de volgende subsecties worden de afzonderlijke PSIRT Security Advisories en de respectieve kwetsbaarheden die in elk

Advies worden behandeld, samengevat:

Cisco TelePresence-endpointapparaten

Niet-geverifieerde CGI-toegang: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan willekeurige code worden uitgevoerd. De aanvalsvector voor exploitatie is via HTTP-pakketten met TCP-poort 8082. Deze kwetsbaarheid is CVE-identificatiecode CVE-2011-0372 toegekend.

CGI Command Injection: Deze kwetsbaarheden kunnen op afstand worden uitgebuit met authenticatie en zonder interactie met de eindgebruiker. Een succesvolle benutting van deze kwetsbaarheden kan de uitvoering van willekeurige codes toestaan. De aanvalsvector voor exploitatie is via misvormde SSL-pakketten (Secure Sockets Layer) met TCP-poort 443. Deze kwetsbaarheden zijn toegewezen CVE-identificatoren CVE-2011-0373, CVE-2011-0374 en CVE-2011-0375.

Openbaarmaking van TFTP-informatie: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder authenticatie en zonder interactie van eindgebruikers. Succesvolle exploitatie van deze kwetsbaarheid kan informatieonthulling toestaan, die een aanvaller in staat stelt om informatie over het getroffen apparaat te leren. De aanvalsvector voor exploitatie is via TFTP GET aanvraagpakketten met UDP-poort 69. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0376.

Injectie van kwaadaardig IP-adres: deze kwetsbaarheid kan op afstand worden uitgebuit zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle benutting van deze kwetsbaarheid kan resulteren in een aanhoudende ontkenning van de dienst (Dos) voorwaarde. De aanvalsvector voor exploitatie is via misvormde Simple Object Access Protocol (SOAP)-pakketten met TCP-poorten 8081 en 9501. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0377.

XML-RPC Command Injection: Deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder authenticatie en zonder interactie van de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan willekeurige code worden uitgevoerd. De aanvalsvector voor exploitatie is via XML-RPC-pakketten met behulp van TCP-poorten 61441 en 61445. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0378.

Cisco Discovery Protocol Remote Code Execution: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan willekeurige code worden uitgevoerd. De aanvalsvector voor exploitatie is via Cisco Discovery Protocol-pakketten. Omdat Cisco Discovery Protocol op de datalink-laag werkt, moet een aanvaller een manier hebben om een frame rechtstreeks naar een getroffen apparaat te verzenden. Dit document zal geen verdere informatie voor deze kwetsbaarheid verstrekken. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0379.

Cisco TelePresence Manager

Bypass voor SOAP-verificatie: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder verificatie en zonder interactie van de eindgebruiker. Succesvolle uitbuiting van deze kwetsbaarheid kan het verheffen van privileges toestaan. De aanvalsvector voor exploitatie is via misvormde SOAP-pakketten met behulp van TCP-poorten 8080 en 8443. Deze kwetsbaarheid is CVE-identificatiecode CVE-2011-0380 toegekend.

Java Remote Method Invocation (RMI) Command Injection: Deze kwetsbaarheid kan op afstand

worden benut zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan willekeurige code worden uitgevoerd. De aanvalsvector voor exploitatie is via gemaakte Java RMI-pakketten met TCP-poorten 1100 en 32000. Deze kwetsbaarheid is CVE-identificatiecode CVE-2011-0381 toegewezen.

Cisco Discovery Protocol Remote Code Execution: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle exploitatie van deze kwetsbaarheid kan willekeurige codeuitvoering toestaan De aanvalsvector voor exploitatie is via Cisco Discovery Protocol-pakketten. Omdat Cisco Discovery Protocol op de datalink-laag werkt, moet een aanvaller een manier hebben om een frame rechtstreeks naar een getroffen apparaat te verzenden. Dit document zal geen verdere informatie voor deze kwetsbaarheid verstrekken. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0379.

Cisco TelePresence Multipoint Switch

Niet-geverifieerde Java Server Access: deze kwetsbaarheden kunnen op afstand worden geëxploiteerd zonder verificatie en zonder interactie van eindgebruikers. Succesvolle uitbuiting van deze kwetsbaarheden kan het opheffen van privileges toestaan. De aanvalsvector voor exploitatie is via gemaakte HTTP-pakketten met TCP-poorten 80 en 8080 en SSL-pakketten met TCP-poort 443. Deze kwetsbaarheden zijn toegewezen CVE-identificatoren CVE-2011-0383 en CVE-2011-0384.

Niet-geverifieerde willekeurige bestanduploadmethode: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan willekeurige code worden uitgevoerd. De aanvalsvector voor exploitatie is via gemaakte HTTP-pakketten met TCP-poort 80 en SSL-pakketten met TCP-poort 443. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0385.

Cisco Discovery Protocol Remote Code Execution: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle exploitatie van deze kwetsbaarheid kan willekeurige codeuitvoering toestaan De aanvalsvector voor exploitatie is via Cisco Discovery Protocol-pakketten. Omdat Cisco Discovery Protocol op de datalink-laag werkt, moet een aanvaller een manier hebben om een frame rechtstreeks naar een getroffen apparaat te verzenden. Dit document zal geen verdere informatie voor deze kwetsbaarheid verstrekken. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0379.

Onbevoegde toegang tot servers: deze kwetsbaarheid kan op afstand worden geëxploiteerd met verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kunnen rechten worden verhoogd. De aanvalsvector voor exploitatie is via HTTP-pakketten met TCP-poort 80 en SSL-pakketten met TCP-poort 443. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0387.

Java RMI Denial of Service: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle benutting van deze kwetsbaarheid kan resulteren in een denial of service-omstandigheid (DoS). Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie. De aanvalsvector voor exploitatie is via gemaakte Java RMI-pakketten via TCP-poort 8999. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0388.

Realtime Transport Control Protocol (RTCP) Denial of Service: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle benutting van deze kwetsbaarheid kan resulteren in een denial of service-omstandigheid (DoS). Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een

aanhoudende DoS-conditie. De aanvalsvector voor exploitatie is via kwaadaardige UDP-pakketten die naar een luisterend RTCP-controlepoort worden gestuurd die willekeurig wordt geselecteerd en besproken tijdens de gespreksinstelling. Een aanvaller kon deze kwetsbaarheid exploiteren met spoofed pakketten. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0389.

XML-RPC Denial of Service: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder authenticatie en zonder interactie van de eindgebruiker. Succesvolle benutting van deze kwetsbaarheid kan resulteren in een denial of service-omstandigheid (DoS). Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie. De aanvalsvector voor exploitatie is via XML-RPC-pakketten met TCP-poort 9000. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0390.

Cisco TelePresence-opnameserver

Niet-geverifieerde Java Servlet Access: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kunnen rechten worden verhoogd. De aanvalsvector voor exploitatie is via gemaakte HTTP-pakketten met TCP-poorten 80 en 8080 en SSL-pakketten met TCP-poort 443. Deze kwetsbaarheid is CVE-identificatiecode CVE-2011-0383 toegekend.

CGI Command Injection: Deze kwetsbaarheid kan op afstand worden uitgebuit zonder authenticatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan willekeurige code worden uitgevoerd. De aanvalsvector voor exploitatie is via SSL-pakketten met TCP-poort 443. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0382.

Niet-geverifieerde willekeurige bestanduploadmethode: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan willekeurige code worden uitgevoerd. De aanvalsvector voor exploitatie is via gemaakte HTTP-pakketten met TCP-poort 80 en SSL-pakketten met TCP-poort 443. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0385.

XML-RPC Arbitrair File Overwrite: Deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder authenticatie en zonder interactie van de eindgebruiker. Succesvolle benutting van deze kwetsbaarheid kan resulteren in een denial of service-omstandigheid (DoS). Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie. De aanvalsvector voor exploitatie is via misvormde XML-RPC-pakketten met behulp van TCP-poorten 12102 en 12104. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0386.

Cisco Discovery Protocol Remote Code Execution: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Als deze kwetsbaarheid met succes wordt benut, kan willekeurige code worden uitgevoerd. De aanvalsvector voor exploitatie is via Cisco Discovery Protocol-pakketten. Omdat Cisco Discovery Protocol op de datalink-laag werkt, moet een aanvaller een manier hebben om een frame rechtstreeks naar een getroffen apparaat te verzenden. Dit document zal geen verdere informatie voor deze kwetsbaarheid verstrekken. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0379.

Ad-hoc-opnamestatus van de service: deze kwetsbaarheid kan op afstand worden geëxploiteerd zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle benutting van deze kwetsbaarheid kan resulteren in een denial of service-omstandigheid (DoS). Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-

conditie. De aanvalsvector voor exploitatie is via HTTP-pakketten met TCP-poort 80. Deze kwetsbaarheid is CVE-identificatiecode CVE-2011-0391 toegewezen.

Java RMI Denial of Service: deze kwetsbaarheid kan op afstand worden benut zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle benutting van deze kwetsbaarheid kan resulteren in een denial of service-omstandigheid (DoS). Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie. De aanvalsvector voor exploitatie is via gemaakte Java RMI-pakketten via TCP-poort 8999. Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0388.

Niet-geverifieerde XML-RPC-interface: deze kwetsbaarheid kan lokaal worden geëxploiteerd zonder verificatie en zonder interactie van de eindgebruiker. Een succesvolle benutting van deze kwetsbaarheid kan leiden tot het uitvoeren van willekeurige acties. De aanvalsvector voor exploitatie is via XML-RPC-pakketten met TCP-poort 8080. Deze kwetsbaarheid is CVE-identificatiecode CVE-2011-0392 toegekend.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de individuele PSIRT Security Advisories, die beschikbaar zijn op de volgende links:

- Meervoudige kwetsbaarheden in Cisco TelePresence-endpointapparaten
- Meervoudige kwetsbaarheden in Cisco TelePresence Manager
- Meervoudige kwetsbaarheden in Cisco TelePresence Multipoint Switch
- Meervoudige kwetsbaarheden in Cisco TelePresence Recording Server

Overzicht Mitigation Technique

Cisco-apparaten bieden verschillende tegenmaatregelen voor deze kwetsbaarheden. 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 vallen, evenals verifiëren het bron IP adres van, pakketten die proberen om deze kwetsbaarheden 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.

Effectieve middelen voor explosiepreventie kunnen ook worden geleverd door de Cisco ASA 5500 Series adaptieve security applicatie en de Cisco Firewall Services Module (FWSM) voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers met het volgende:

- Toegangscontrolelijsten voor douanevervoer (ACL's)

- Unicast RPF

Deze beschermingsmechanismen filteren en vallen, evenals verifiëren het bron IP adres van, pakketten die proberen om deze kwetsbaarheden te exploiteren.

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

Raadpleeg de Cisco TelePresence Hardening Guide voor extra informatie over de verschillende aspecten die u moet overwegen bij het beveiligen van een Cisco TelePresence-omgeving.

Risicobeheer

Organisaties wordt aangeraden hun standaard risicobeoordelings- en risicobeperkingsprocessen te volgen om de potentiële impact van deze kwetsbaarheden 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 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 kwetsbaarheden bieden wanneer de aanval afkomstig is van een vertrouwd bronadres.

Het iACL-beleid ontkent de pakketten op de volgende protocollen/poorten die naar getroffen apparaten worden verzonden:

- TCP-poort 80
- TCP-poort 443
- TCP-poort 1100
- TCP-poort 8080
- TCP-poort 8081
- TCP-poort 8082
- TCP-poort 8443
- TCP-poort 8999
- TCP-poort 9000
- TCP-poort 9501
- TCP-12102
- TCP-12104
- TCP-32000
- TCP-61441
- TCP-61445
- UDP-poort 69

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 ports ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 80
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 1100 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 8080 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 8081 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8082 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 8999 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 9000 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9501 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 12102 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 12104 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
```

```
eq 32000 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61441 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61445 permit udp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 69 ! !-- The following vulnerability-specific access
control entries !-- (ACEs) can aid in identification of attacks ! deny tcp any
192.168.60.0 0.0.0.255 eq 80 deny tcp any 192.168.60.0 0.0.0.255 eq 443 deny tcp any
192.168.60.0 0.0.0.255 eq 1100 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 deny tcp
any 192.168.60.0 0.0.0.255 eq 8081 deny tcp any 192.168.60.0 0.0.0.255 eq 8082 deny
tcp any 192.168.60.0 0.0.0.255 eq 8443 deny tcp any 192.168.60.0 0.0.0.255 eq 8999
deny tcp any 192.168.60.0 0.0.0.255 eq 9000 deny tcp any 192.168.60.0 0.0.0.255 eq
9501 deny tcp any 192.168.60.0 0.0.0.255 eq 12102 deny tcp any 192.168.60.0 0.0.0.255
eq 12104 deny tcp any 192.168.60.0 0.0.0.255 eq 32000 deny tcp any 192.168.60.0
0.0.0.255 eq 61441 deny tcp any 192.168.60.0 0.0.0.255 eq 61445 deny udp any
192.168.60.0 0.0.0.255 eq 69 ! !-- 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-onbereikbaarheid. ICMP onbereikbare snelheidsbeperking kan worden gewijzigd van de standaard met behulp van de globale configuratie commando ip icmp snelheid-limiet onbereikbare interval-in-ms.

Beperken: bescherming tegen spoofing

Unicast doorsturen van omgekeerde paden

Een van de kwetsbaarheden die in dit document worden 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, raadpleegt u 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 kwetsbaarheden die in dit document worden 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 de pakketten op de volgende protocollen/poorten identificeren die zijn gefilterd op interfaces waarop iACL wordt toegepast:

- TCP-poort 80
- TCP-poort 443
- TCP-poort 1100
- TCP-poort 8080
- TCP-poort 8081
- TCP-poort 8082
- TCP-poort 8443
- TCP-poort 8999
- TCP-poort 9000
- TCP-poort 9501
- TCP-12102
- TCP-12104
- TCP-32000
- TCP-61441
- TCP-61445
- UDP-poort 69

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 volgt:

```
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 www
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    30 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1100
    40 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
    50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8081
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8082
    70 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 (1 match)
    80 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8999
    90 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9000
    100 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9501
    110 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 12102
    120 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 12104
    130 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 32000
    140 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61441
    150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61445
    160 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq tftp
```

```
    170 deny tcp any 192.168.60.0 0.0.0.255 eq www (703 matches)
    180 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (213 matches)
    190 deny tcp any 192.168.60.0 0.0.0.255 eq 1100 (95 matches)
    200 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 (115 matches)
    210 deny tcp any 192.168.60.0 0.0.0.255 eq 8081 (119 matches)
    220 deny tcp any 192.168.60.0 0.0.0.255 eq 8082 (86 matches)
    230 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (125 matches)
    240 deny tcp any 192.168.60.0 0.0.0.255 eq 8999 (63 matches)
    250 deny tcp any 192.168.60.0 0.0.0.255 eq 9000 (3 matches)
    260 deny tcp any 192.168.60.0 0.0.0.255 eq 9501 (142 matches)
    270 deny tcp any 192.168.60.0 0.0.0.255 eq 12102 (127 matches)
    280 deny tcp any 192.168.60.0 0.0.0.255 eq 12104 (132 matches)
    290 deny tcp any 192.168.60.0 0.0.0.255 eq 32000 (125 matches)
    300 deny tcp any 192.168.60.0 0.0.0.255 eq 61441 (110 matches)
    310 deny tcp any 192.168.60.0 0.0.0.255 eq 61445 (114 matches)
    320 deny udp any 192.168.60.0 0.0.0.255 eq tftp (218 matches)
    330 deny ip any 192.168.60.0 0.0.0.255 (9 matches)
router#
```

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

- 703 HTTP-pakketten op TCP-poort 80 (www) voor ACE-lijn 170
- 213 SSL-pakketten op TCP-poort 443 voor ACE-lijn 180
- 95 pakketten op TCP-poort 1100 voor ACE-lijn 190
- 115 pakketten op TCP-poort 8080 voor ACE-lijn 200
- 119 pakketten op TCP-poort 8081 voor ACE-lijn 210
- 86 pakketten op TCP-poort 8082 voor ACE-lijn 220
- 125 pakketten op TCP-poort 8443 voor ACE-lijn 230
- 63 pakketten op TCP-poort 8999 voor ACE-lijn 240
- 3 pakketten op TCP-poort 9000 voor ACE-lijn 250
- 142 pakketten op TCP-poort 9501 voor ACE-lijn 260
- 127 pakketten op TCP-12102 voor ACE-lijn 270
- 132 pakketten op TCP-12104 voor ACE-lijn 280
- 125 pakketten op TCP-32000 voor ACE-lijn 290
- 110 pakketten op TCP-61441 voor ACE-lijn 300
- 114 pakketten op TCP-61445 voor ACE-lijn 310
- 218 TFTP-pakketten op UDP-poort 69 voor ACE-lijn 320

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-ingangstoegangscontrolelijst (ACL) zorgt ervoor dat pakketten die overeenkomen met specifieke ACE's worden vastgelegd. De log-input optie maakt het registreren van de ingangsinterface 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 ip-toegangslijst met interval-in-ms voor vastlegging de effecten van processwitching beperken die worden geïnduceerd door ACL-vastlegging. De opdracht logsnelheid-limiet rate-per-seconde [behalve loglevel] beperkt het effect van het genereren en verzenden van logbestanden.

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 show cef interface type sleuf/poort 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-softwareversie 12.4(20)T is de opdracht **tonen dat ip cef switching** is vervangen door **toon ip cef switching statistieken eigenschap**.

Opmerking: de opdracht **show | Start** regex en **toon** opdracht **| inclusief** regex-opdrachtaanpassingen die in de volgende voorbeelden worden gebruikt om de hoeveelheid uitvoer te minimaliseren die beheerders moeten parseren om de gewenste informatie te bekijken. Er is aanvullende informatie over opdrachtbepalingen in de secties met 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 voorgaande **show cef drop**, **toon ip cef switching statistieken functie** en **toon ip traffic** voorbeelden, Unicast RPF heeft laten vallen **18 IP 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 mogelijk pogingen zijn om deze kwetsbaarheden te exploiteren. De beheerders worden geadviseerd om stromen te onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren of of zij wettige verkeersstromen zijn.

```
router#show ip cache flow

IP packet size distribution (1779 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .323 .676 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

IP Flow Switching Cache, 278544 bytes
  183 active, 3913 inactive, 364 added
  4883 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW             16      0.0         7    40      0.0       0.0      15.7
TCP-other          126      0.0         3    40      0.1       0.0      15.4
UDP-TFTP             7      0.0         6    28      0.0       0.0      15.6
UDP-other           32      0.0         6    28      0.0       0.0      15.4
Total:             181      0.0         4    36      0.1       0.0      15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.21.36   Et0/1         192.168.60.17   11 CD3E 0045     1
```

```
Et0/0         192.168.100.31  Et0/1         192.168.60.210  06 8F8C 044C     6
Et0/0         192.168.100.14  Et0/1         192.168.60.121  06 DEBB 251D     3
Et0/0         192.168.100.209 Et0/1         192.168.60.19   06 C460 1F90     3
Et0/0         192.168.100.235 Et0/1         192.168.60.15   06 46E6 7D00     1
Et0/0         192.168.159.166 Et0/1         192.168.90.53   11 62E2 B413    10
Et0/0         192.168.100.164 Et0/1         192.168.60.91   06 5460 2F46     3
Et0/0         192.168.100.83  Et0/1         192.168.60.30   06 E440 1F92     6
Et0/0         192.168.12.204  Et0/1         192.168.162.10  11 39D3 9273    10
Et0/0         192.168.100.211 Et0/1         192.168.60.174  06 846A 1F91     4
Et0/0         192.168.100.112 Et0/1         192.168.60.242  06 4F39 044C     3
Et0/0         192.168.100.147 Et0/1         192.168.60.153  06 9B55 0050    15
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2327     4
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2328     4
Et0/0         192.168.194.210 Et0/1         192.168.4.64    11 85DE BE0C     5
Et0/0         192.168.100.171 Et0/1         192.168.60.215  06 84F3 1F91     1
Et0/0         192.168.100.121 Et0/1         192.168.60.165  06 15A0 2F48     8
Et0/0         192.168.100.97  Et0/1         192.168.60.22   06 0951 2327     1
Et0/0         192.168.100.221 Et0/1         192.168.60.170  06 DBCF 0050    10
Et0/0         192.168.6.90    Et0/1         192.168.243.120 06 14E7 773D    10
Et0/0         192.168.100.174 Et0/1         192.168.60.239  06 0414 1F91     5
Et0/0         192.168.100.51  Et0/1         192.168.60.109  06 EF9D 251D     2
Et0/0         192.168.78.53   Et0/1         192.168.60.37   11 07A2 0045     2
Et0/0         192.168.164.19  Et0/1         192.168.201.180 06 FA1C 557B     5
Et0/0         192.168.66.15   Et0/1         192.168.155.182 11 FBC6 585A     3
Et0/0         192.168.100.208 Et0/1         192.168.60.137  06 BEC3 20FB     1
Et0/0         192.168.100.43  Et0/1         192.168.60.70   06 5E31 01BB    14
Et0/0         192.168.100.43  Et0/1         192.168.60.0    06 0FAA F001     1
Et0/0         192.168.29.205  Et0/1         192.168.240.249 11 71B3 8F9C     8
Et0/0         192.168.100.179 Et0/1         192.168.60.214  06 A2C4 F005     4
Et0/0         192.168.89.13   Et0/1         192.168.204.26  11 1D17 2CB0    11
router#
```

In het bovenstaande voorbeeld zijn er meerdere stromen voor:

- HTTP op TCP-poort 80 (hex-waarde 0050)
- SSL op TCP-poort 443 (hex-waarde 101B)
- TCP-poort 1100 (hex-waarde 044C)
- TCP-poort 8080 (hex-waarde 1F90)
- TCP-poort 8081 (hex-waarde 1F91)
- TCP-poort 8082 (hex-waarde 1F92)
- TCP-poort 8443 (hex-waarde 20FB)
- TCP-poort 8999 (hex-waarde 2327)
- TCP-poort 9000 (hex-waarde 2328)
- TCP-poort 9501 (hex-waarde 251D)
- TCP-12102 (hex-waarde 2F46)
- TCP-12104 (hex-waarde 2F48)
- TCP-32000 (hex-waarde 7D00)
- TCP-61441 (hex-waarde F001)
- TCP-61445 (hex-waarde F005)
- TFTP op UDP-poort 69 (hex-waarde 0045)

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 kwetsbaarheden te exploiteren. De beheerders worden geadviseerd om deze stromen bij basislijngebruik voor verkeer te vergelijken dat op de bovengenoemde protocollen/de havens wordt verzonden en ook de stromen te onderzoeken om te bepalen of zij van onbetrouwbare gastheren of netwerken afkomstig zijn. Om

alleen de verkeersstromen voor pakketten op de bovengenoemde poorten/protocollen te bekijken, toont de opdracht ip cache flow | omvat SrcIf|__11_.*0045 zal de verwante verslagen van UDP NetFlow zoals hier getoond tonen:

UDP-stromen

```
router#show ip cache flow | include SrcIf|_11_.*0045
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

Et0/0         192.168.54.222  Et0/1         192.168.60.43   11 7947 0045     3
Et0/0         192.168.247.117 Et0/1         192.168.60.169  11 45FB 0045     1
Et0/0         192.168.250.16  Et0/1         192.168.60.79   11 66AC 0045    10
Et0/0         192.168.121.112 Et0/1         192.168.60.36   11 6725 0045    16
Et0/0         192.168.243.192 Et0/1         192.168.60.225  11 2B52 0045     1
router#
```

Om alleen de verkeersstromen voor pakketten op de bovengenoemde poorten/protocollen te bekijken, toont de opdracht ip cache flow | omvat SrcIf|__06_.*(0050|01BB|044C|1F90|1F91|1F92|20FB|2327|2328|251D|2F46|2F48|7D00|F001|F005)_ zal de verwante TCP NetFlow-records weergeven zoals hieronder wordt getoond:

TCP-stromen

```
router#show ip cache flow | include
SrcIf|_06_.*(0050|01BB|044C|1F90|1F91|1F92|20FB|2327|2328|251D|2F46|2F48|7D00|F001|F0
05)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.100.14  Et0/1          192.168.60.121  06 DEBB 251D     3
Et0/0         192.168.100.209 Et0/1          192.168.60.19   06 C460 1F90     3
Et0/0         192.168.100.235 Et0/1          192.168.60.15   06 46E6 7D00     1
Et0/0         192.168.100.164 Et0/1          192.168.60.91   06 5460 2F46     3
Et0/0         192.168.100.83  Et0/1          192.168.60.30   06 E440 1F92     6

Et0/0         192.168.100.211 Et0/1          192.168.60.174  06 846A 1F91     4
Et0/0         192.168.100.112 Et0/1          192.168.60.242  06 4F39 044C     3
Et0/0         192.168.100.147 Et0/1          192.168.60.153  06 9B55 0050    15
Et0/0         192.168.100.188 Et0/1          192.168.60.26   06 E9AC 2327     4
Et0/0         192.168.100.188 Et0/1          192.168.60.26   06 E9AC 2328     4

Et0/0         192.168.100.121 Et0/1          192.168.60.165  06 15A0 2F48     8

Et0/0         192.168.100.208 Et0/1          192.168.60.137  06 BEC3 20FB     1
Et0/0         192.168.100.43  Et0/1          192.168.60.70   06 5E31 01BB    14
Et0/0         192.168.100.43  Et0/1          192.168.60.0    06 0FAA F001     1
Et0/0         192.168.100.179 Et0/1          192.168.60.214  06 A2C4 F005     4

Et0/0         192.168.100.209 Et0/1          192.168.60.19   06 C460 1F90     3
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 kwetsbaarheden bieden wanneer de aanval afkomstig is van een vertrouwd bronadres.

Het tACL-beleid ontkent de pakketten op de volgende protocollen/poorten die naar getroffen apparaten worden verzonden:

- TCP-poort 80
- TCP-poort 443
- TCP-poort 1100
- TCP-poort 8080
- TCP-poort 8081
- TCP-poort 8082
- TCP-poort 8443
- TCP-poort 8999
- TCP-poort 9000
- TCP-poort 9501
- TCP-12102
- TCP-12104
- TCP-32000
- TCP-61441
- TCP-61445
- UDP-poort 69

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 ports ! access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 80 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 443 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 1100
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8080 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8081 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 8082 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8443 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8999
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 9000 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9501 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 12102 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 12104 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 32000
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 61441 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61445 access-list tACL-Policy extended permit udp host
```

```
192.168.100.1 192.168.60.0 255.255.255.0 eq 69 ! !-- The following vulnerability-
specific access control entries !-- (ACEs) can aid in identification of attacks !
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 80
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 1100
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8080
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8081
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8082
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8999
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 9000
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 9501
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 12102
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 12104
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 32000
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 61441
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 61445
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 69 ! !--
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 kwetsbaarheden die in dit document worden beschreven, kunnen 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 Cisco Security Appliance Command Reference voor IP-verificatie van het omgekeerde pad en het Understanding Unicast Reverse Path Forwarding Applied Intelligence-witboek.

Identificatie: Toegangscontrolelijsten voor douanevervoer

Nadat tACL is toegepast op een interface, kunnen beheerders het bevel van de show access-list gebruiken om de volgende protocollen/poorten te identificeren die zijn gefilterd:

- TCP-poort 80
- TCP-poort 443
- TCP-poort 1100
- TCP-poort 8080
- TCP-poort 8081
- TCP-poort 8082
- TCP-poort 8443
- TCP-poort 8999
- TCP-poort 9000

- TCP-poort 9501
- TCP-12102
- TCP-12104
- TCP-32000
- TCP-61441
- TCP-61445
- UDP-poort 69

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 tACL-Beleid volgt:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 31 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq www (hitcnt=55)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq https (hitcnt=765)
access-list tACL-Policy line 3 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 1100 (hitcnt=43)
access-list tACL-Policy line 4 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8080 (hitcnt=265)
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8081 (hitcnt=18)
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8082 (hitcnt=77)
access-list tACL-Policy line 7 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8443 (hitcnt=345)
access-list tACL-Policy line 8 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8999 (hitcnt=137)
access-list tACL-Policy line 9 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9000 (hitcnt=17)
access-list tACL-Policy line 10 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9501 (hitcnt=36)
access-list tACL-Policy line 11 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 12102 (hitcnt=40)
access-list tACL-Policy line 12 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 12104 (hitcnt=23)
access-list tACL-Policy line 13 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 32000 (hitcnt=109)
access-list tACL-Policy line 14 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61441 (hitcnt=60)
access-list tACL-Policy line 15 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61445 (hitcnt=95)
access-list tACL-Policy line 16 extended permit udp host 192.168.100.1
192.168.60.0 255.255.255.0 eq tftp (hitcnt=4567)
access-list tACL-Policy line 17 extended deny tcp any
192.168.60.0 255.255.255.0 eq www (hitcnt=28)
access-list tACL-Policy line 18 extended deny tcp any
192.168.60.0 255.255.255.0 eq https (hitcnt=169)
access-list tACL-Policy line 19 extended deny tcp any
192.168.60.0 255.255.255.0 eq 1100 (hitcnt=93)
access-list tACL-Policy line 20 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8080 (hitcnt=11)
access-list tACL-Policy line 21 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8081 (hitcnt=9)
access-list tACL-Policy line 22 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8082 (hitcnt=9)
```

```
access-list tACL-Policy line 23 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8443 (hitcnt=34)
access-list tACL-Policy line 24 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8999 (hitcnt=46)
access-list tACL-Policy line 25 extended deny tcp any
192.168.60.0 255.255.255.0 eq 9000 (hitcnt=6)
access-list tACL-Policy line 26 extended deny tcp any
192.168.60.0 255.255.255.0 eq 9501 (hitcnt=9)
access-list tACL-Policy line 27 extended deny tcp any
192.168.60.0 255.255.255.0 eq 12102 (hitcnt=11)
access-list tACL-Policy line 28 extended deny tcp any
192.168.60.0 255.255.255.0 eq 12104 (hitcnt=24)
access-list tACL-Policy line 29 extended deny tcp any
192.168.60.0 255.255.255.0 eq 32000 (hitcnt=48)
access-list tACL-Policy line 30 extended deny tcp any
192.168.60.0 255.255.255.0 eq 61441 (hitcnt=32)
access-list tACL-Policy line 31 extended deny tcp any
192.168.60.0 255.255.255.0 eq 61445 (hitcnt=9)
access-list tACL-Policy line 32 extended deny udp any
192.168.60.0 255.255.255.0 eq tftp (hitcnt=78)
access-list tACL-Policy line 33 extended deny ip any any (hitcnt=4658)
firewall#
```

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

- 28 HTTP-pakketten op TCP-poort 80 (www) voor ACE-lijn 17
- 169 SSL-pakketten op TCP-poort 443 (https) voor ACE-lijn 18
- 93 pakketten op TCP-poort 1100 voor ACE-lijn 19
- 11 pakketten op TCP-poort 8080 voor ACE-lijn 20
- 9 pakketten op TCP-poort 8081 voor ACE-lijn 21
- 9 pakketten op TCP-poort 8082 voor ACE-lijn 22
- 34 pakketten op TCP-poort 8443 voor ACE-lijn 23
- 46 pakketten op TCP-poort 8999 voor ACE-lijn 24
- 6 pakketten op TCP-poort 9000 voor ACE-lijn 25
- 9 pakketten op TCP-poort 9501 voor ACE-lijn 26
- 11 pakketten op TCP-12102 voor ACE-lijn 27
- 24 pakketten op TCP-12014 voor ACE-lijn 28
- 48 pakketten op TCP-32000 voor ACE-lijn 29
- 32 pakketten op TCP-61441 voor ACE-lijn 30
- 9 pakketten op TCP-61445 voor ACE-lijn 31
- 78 TFTP-pakketten op UDP-poort 69 (tftp) voor ACE-lijn 32

Identificatie: berichten in Firewall Access List System

Het 106023 van het firewallsyslog zal voor pakketten worden geproduceerd die door een toegangscontroleingang (ACE) worden ontkend die niet het aanwezige logboeksleutelwoord 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 kwetsbaarheden te exploiteren die in dit document worden beschreven. Het is mogelijk om verschillende reguliere expressies te gebruiken met het sleutelwoord grep om te zoeken naar specifieke gegevens in de gelogde berichten.

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

```
firewall#show logging | grep 106023
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.215/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.173/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.225.47/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.156.169/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.191.223/1024
                  dst inside:192.168.60.103/8080 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/8080 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.177/8080 by access-group "tACL-Policy"
firewall#
```

In het voorafgaande voorbeeld, tonen de berichten die voor tACL tACL-Policy worden geregistreerd HTTP-pakketten voor TCP-poort 80, SSL-pakketten voor TCP-poort 443, pakketten voor TCP-poort 1100 en pakketten voor TCP-poort 8080 die naar het adresblok worden gestuurd dat aan de betreffende apparaten 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 Using Firewall en IOS Router Syslog Events Applied Intelligence.

Identificatie: bescherming tegen spoofing met Unicast Reverse Path Forwarding

106021 wordt gegenereerd voor pakketten die worden geweigerd door Unicast RPF. 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 kwetsbaarheden te exploiteren die in dit document worden 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 106021
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
        Feb 21 2010 00:15:13: %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-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, verwijzen we naar de Cisco Security Appliance Command Reference voor show asp drop.

Cisco-inbraakpreventiesysteem

Beperken: acties voor Cisco IPS-handtekeningen

Beheerders kunnen Cisco Inbraakpreventiesysteem (IPS) gebruiken om bedreigingsdetectie te bieden en pogingen te voorkomen om de kwetsbaarheden te exploiteren die in dit document worden beschreven. Deze kwetsbaarheden kunnen door de volgende handtekeningen worden gedetecteerd:

- 32719-0: Uitvoeren van Cisco TelePresence niet-geverifieerde externe willekeurige

opdracht
- 33859-0: Cisco TelePresence Endpoint voor CGI-opdrachtinjectie
- 33860-0: Cisco TelePresence Multipoint Switch Java Server Access
- 33860-1: Cisco TelePresence Multipoint Switch Java Server Access
- 33861-0: Kwetsbaarheid voor uitvoering van opdrachten voor Cisco TelePresence Opnameserver

32719-0: Uitvoeren van Cisco TelePresence niet-geverifieerde externe willekeurige opdracht

Beginnend met handtekeningsupdate S550 voor sensoren met Cisco IPS versie 6.x en hoger, kunnen deze kwetsbaarheden worden gedetecteerd door handtekening 32719/0 (Handtekeningnaam: Cisco TelePresence Unauthenticated Remote Arbitary Command Execution). Signature 32719/0 is standaard ingeschakeld, activeert een gebeurtenis met hoge ernst, heeft een SFR (Signature fidelity rating) van 90 en is geconfigureerd met een **automatische waarschuwing** voor de gebeurtenis.

Vuren van handtekening 32719/0 op een poging om een niet-geverifieerde externe kwetsbaarheid voor de uitvoering van willekeurige opdrachten te exploiteren in een Cisco TelePresence Endpoint dat is verzonden met TCP-poort 8082. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van deze kwetsbaarheden.

33859-0: Cisco TelePresence Endpoint voor CGI-opdrachtinjectie

Beginnend met handtekeningsupdate S550 voor sensoren waarop Cisco IPS versie 6.x en hoger wordt uitgevoerd, kunnen deze kwetsbaarheden worden gedetecteerd door handtekening 33859-0 (Signature Name: Cisco TelePresence Endpoint CGI Command Injection). Signature 33859/0 is standaard ingeschakeld, activeert een gebeurtenis met hoge ernst, heeft een SFR (Signature fidelity rating) van 80 en is geconfigureerd met een **automatische waarschuwing** voor de gebeurtenis.

Vuren van handtekening 33859/0 op een poging om een niet-geverifieerde externe kwetsbaarheid voor de uitvoering van willekeurige opdrachten te exploiteren in een Cisco TelePresence Endpoint dat is verzonden met TCP-poort 8082. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van deze kwetsbaarheden.

33860-0: Cisco TelePresence Multipoint Switch Java Server Access

Beginnend met handtekeningsupdate S550 voor sensoren waarop Cisco IPS versie 6.x en hoger wordt uitgevoerd, kunnen deze kwetsbaarheden worden gedetecteerd door handtekening 33860-0 (Signature Name: Cisco TelePresence Multipoint Switch Java Server Access). Handtekening 33860/0 is standaard uitgeschakeld, activeert een gebeurtenis met hoge ernst, heeft een SFR (Signature Fidelity Rating) van 75 en is geconfigureerd met een **automatische** gebeurtenis-**waarschuwing**.

Vuren van handtekening 33860/0 bij het detecteren van de toegang van meerdere Java-servers binnen de Cisco TelePresence Multipoint Switch die is verzonden via TCP-poort 8080. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van deze kwetsbaarheden.

Opmerking: deze handtekening kan handig branden op apparaten die geen Cisco TelePresence Multipoint Switches zijn. Er is verder onderzoek nodig om dergelijke apparatuur te elimineren.

33860-1: Cisco TelePresence Multipoint Switch Java Server Access

Beginnend met handtekeningsupdate S550 voor sensoren waarop Cisco IPS versie 6.x en hoger wordt uitgevoerd, kunnen deze kwetsbaarheden worden gedetecteerd door handtekening 33860-1 (Signature Name: Cisco TelePresence Multipoint Switch Java Server Access). Handtekening 33860/1 is standaard uitgeschakeld, activeert een gebeurtenis met hoge ernst, heeft een SFR (Signature Fidelity Rating) van 75 en is geconfigureerd met een **automatische** gebeurtenis-**waarschuwing**.

Vuren van handtekening 33860/1 na het detecteren van de toegang van meerdere Java-servers binnen de Cisco TelePresence Multipoint Switch die is verzonden via TCP-poort 80. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van deze kwetsbaarheden.

Opmerking: deze handtekening kan handig branden op apparaten die geen Cisco TelePresence Multipoint Switches zijn. Er is verder onderzoek nodig om dergelijke apparatuur te elimineren.

33861-0: Kwetsbaarheid voor uitvoering van opdrachten voor Cisco TelePresence Opnameserver

Beginnend met handtekeningupdate S550 voor sensoren met Cisco IPS versie 6.x en hoger, kunnen deze kwetsbaarheden worden gedetecteerd door handtekening 33861/0 (Handtekeningnaam: Cisco TelePresence Recording Server Command Execution Vulnerability). Signature 33861/0 is standaard ingeschakeld, activeert een gebeurtenis met hoge ernst, heeft een SFR (Signature fidelity rating) van 90 en is geconfigureerd met een **automatische waarschuwing** voor de gebeurtenis.

Deze handtekening brandt bij het detecteren van een poging om een specifieke kwetsbaarheid voor opdrachtuitvoering in Cisco TelePresence Recording Server te exploiteren. Deze kwetsbaarheid is verder gedocumenteerd in CVE-2011-0382.

Handtekening 33861/0 is een meta-handtekening en bestaat uit meerdere onderhandtekeningen (Signature IDs 33861-1 tot en met 33861-4) die allemaal moeten worden geactiveerd om de meta-handtekening te activeren. Elk van de individuele ondertekenaars heeft daarom geen evenement actie op zich en dus wordt elk beschouwd als een Informationele ernstgebeurtenis.

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 kwetsbaarheden te exploiteren die in dit document worden 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 kwetsbaarheden te exploiteren die in dit document worden 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 zijn gerelateerd aan de kwetsbaarheden die in dit document worden beschreven met behulp van IPS-handtekeningen:

- 32719-0: Uitvoeren van Cisco TelePresence niet-geverifieerde externe willekeurige opdracht
- 33859-0: Cisco TelePresence Endpoint voor CGI-opdrachtinjectie
- 33860-0: Cisco TelePresence Multipoint Switch Java Server Access
- 33860-1: Cisco TelePresence Multipoint Switch Java Server Access
- 33861-0: Kwetsbaarheid voor uitvoering van opdrachten voor Cisco TelePresence Opnameserver

Nadat de dynamische handtekeningupdate S550 is gedownload, zal het gebruik van de volgende trefwoorden voor de respectievelijke IPS handtekeningen-ID's en een vraagtype van **All Matching Event Raw Messages** op het Cisco Security MARS-apparaat een rapport leveren met een lijst van de incidenten die door de IPS-handtekening zijn gemaakt.

- **NR-32719/0** voor IPS-handtekeningen 32719/0
- **NR-33859/0** voor IPS-handtekeningen 33859/0
- **NR-33860/0** voor IPS-handtekeningen 33860/0
- **NR-33860/1** voor IPS-handtekeningen 33860/1
- **NR-3861** voor IPS-handtekeningen 33861/0 tot en met 33861/4

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 weergegeven. 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 van de versie van IPS-handtekeningen 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 1.1	2011-februari-25	Bijgewerkt om informatie op Handtekening-ID 33861-0 op te nemen.
Revisie 1.0	2011-februari-23	Eerste publieke 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 TelePresence harde onderhoudshandleiding
- Cisco-bulletins voor toegepaste beperking
- Cisco-beveiliging
- Cisco Security IntelliShield Alert Manager-service
- Cisco-handleiding over het versterken van Cisco IOS-apparaten
- De betekenis van cross-site scripting (XSS) bedreigingsvectoren
- 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
- Opdrachttaal voor gereedschap beveiligen op Cisco IOS
- Cisco Firewallproducten - startpagina op Cisco.com
- Cisco ACE-documentatie voor Application Control Engine
- Verbeteringen in Unicast Reverse Path Forwarding voor de Internet Service Provider
- 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.