Identificatie en beperking van de exploitatie van de kwetsbaarheid in CiscoWorks Common Services

Identificatie en beperking van de exploitatie van de kwetsbaarheid in CiscoWorks Common Services

Advies-ID: cisco-amb-20101027-cs

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20101027-cs

Revisie 1.0

Openbare publicatie 2010 oktober 27 16:00 UTC (GMT)

Inhoud

Cisco Response

Dit Toegepaste Mitigation Bulletin is een begeleidend document bij de kwetsbaarheid voor *implementatie van* PSIRT Security Advisory *CiscoWorks Common Services Arbitary Code Execution* en biedt identificatie- en mitigatietechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

Cisco Common Services voor CiscoWorks bevat een kwetsbaarheid wanneer een misvormd pakket wordt verwerkt. Deze kwetsbaarheid kan op afstand worden uitgebuit zonder verificatie en zonder interactie met de eindgebruiker. Succesvolle exploitatie van deze kwetsbaarheid kan willekeurige code uitvoering toestaan, of kan het beïnvloede apparaat veroorzaken om te crashen. De aanvalsvector voor exploitatie is door pakketten die TCP-poort 443 en TCP-poort 1741 gebruiken wanneer de standaardconfiguratie wordt gebruikt.

Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2010-3036.

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-20101027-cs.

Overzicht Mitigation Technique

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

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

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

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

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

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

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

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

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

Risicobeheer

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

Apparaatspecifieke beperking en identificatie

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

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

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

Cisco IOS-routers en -Switches

Beperking: toegangscontrolelijsten voor douanevervoer

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

Het tACL-beleid ontkent onbevoegde pakketten op de standaardpoorten, TCP-poort 443 en TCP-poort 1741, die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 is de IP adresruimte die door de beïnvloede apparaten wordt gebruikt, en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend.

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

```
!-- Include explicit permit statements for trusted sources !-- that require access on
the vulnerable ports ! access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 443 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 1741 ! !-- The following vulnerability-specific access control entries !-- (ACEs)
can aid in identification of attacks ! access-list 150 deny tcp any 192.168.60.0
0.0.0.255 eq 443 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 1741 ! !--
Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing
security policies and configurations ! !-- Explicit deny for all other IP traffic !
access-list 150 deny ip any any ! !-- Apply tACL to interfaces in the ingress
direction ! interface GigabitEthernet0/0 ip access-group 150 in
```

Merk op dat het filtreren met een lijst van de interfacetoegang de transmissie van onbereikbare berichten ICMP terug naar de bron van het gefilterde verkeer zal veroorzaken. Het genereren van deze berichten zou het ongewenste effect kunnen hebben van het verhogen van CPU-gebruik op het apparaat. In Cisco IOS-software is de onbereikbare ICMP-generatie standaard beperkt tot één pakket per 500 milliseconden. ICMP onbereikbare berichtgeneratie kan worden uitgeschakeld met

de opdracht interfaceconfiguratie **zonder IP-onbereikbaar**. ICMP-onbereikbare snelheidsbeperking kan worden gewijzigd ten opzichte van de standaardinstelling met behulp van de **algemene** opdracht voor configuratie **ip icmp-snelheidslimiet voor onbereikbare** *interval-in-ms*.

Identificatie: Toegangscontrolelijsten voor douanevervoer

Nadat de beheerder de tACL op een interface heeft toegepast, zal de opdracht **IP-toegangslijsten tonen** het aantal pakketten op TCP-poort 443 en TCP-poort 1741 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 ip toegang-lijsten 150** volgt:

```
router#show ip access-lists 150
Extended IP access list 150
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1741
    30 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (12 matches)
    40 deny tcp any 192.168.60.0 0.0.0.255 eq 1741 (26 matches)
    50 deny ip any any
router#
```

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

- **12** pakketten op **TCP-poort 443** voor ACE-lijn 30
- **26** pakketten op **TCP-poort 1741** voor ACE-lijn 40

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

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

Identificatie: Vastlegging toegangslijst

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

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

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

De CPU-impact van ACL-vastlegging kan worden aangepakt in hardware op de Cisco Catalyst

6500 Series-switches en Cisco 7600 Series-routers met Supervisor Engine 720 of Supervisor Engine 32 met behulp van geoptimaliseerde ACL-vastlegging.

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

Cisco IOS NetFlow

Identificatie: Traffic Flow Identification met NetFlow-records

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

```
router#show ip cache flow
IP packet size distribution (17258967 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .013 .225 .422 .155 .035 .008 .005 .004 .002 .001 .014 .002 .002 .003 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .045 .017 .034 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  18 active, 65518 inactive, 2445817 added
  226043591 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 533256 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         653      0.0        77    40      0.0      27.4      24.0
TCP-FTP            765      0.0        15    42      0.0       1.3      25.8
TCP-FTPD             3      0.0       324   608      0.0       1.9      42.9
TCP-WWW          43844      0.0        20   456      0.2       9.3      40.0
TCP-SMTP          4973      0.0         6    59      0.0      35.3      59.7
TCP-X                2      0.0         1    52      0.0       0.0      66.8
TCP-BGP              2      0.0         1    52      0.0       0.0      63.7
TCP-NNTP             2      0.0         1    52      0.0       0.0      88.7
TCP-other       276300      0.0        19   267      1.2      29.1      41.8
UDP-DNS         236963      0.0         2    69      0.1       8.8      57.8
UDP-NTP          31121      0.0         1    75      0.0       0.2      60.3
UDP-TFTP             9      0.0         4    80      0.0      27.6      55.7
UDP-other       485427      0.1         8   106      0.9      21.6      56.4
ICMP            642287      0.1         2    83      0.3      10.6      60.0
IGMP            265863      0.0         2    37      0.1      53.9      42.7
IP-other        457584      0.1         8    92      0.9      94.0      16.3
Total:         2445798      0.5         7   167      4.0      34.9      46.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.137.50  Gi0/1         192.168.60.42   11 0984 00A1     1
Gi0/0         192.168.211.3   Gi0/1         192.168.60.101  11 0911 00A1     3
Gi0/0         192.168.18.79   Gi0/1         192.168.60.105  06 1C16 06CD     4
```

```
Gi0/0          192.168.203.49  Gi0/1          192.168.60.67   11 0B3E 00A1     5
Gi0/0          192.168.101.251 Gi0/1          192.168.60.103  06 3A89 01BB     1
Gi0/0          192.168.122.5   Gi0/1          192.168.60.29   11 0BD7 00A1     1
Gi0/0          192.168.40.131  Gi0/1          192.168.60.80   06 22FC 01BB     7
router#
```

In het bovenstaande voorbeeld zijn er meerdere stromen op **TCP**-poort **443 (hex-waarde 01B)** en **TCP**-poort **1741 (hex-waarde 06CD)**.

Om alleen de verkeersstromen voor pakketten op TCP-poort 443 (hex-waarde 01B) en TCP-poort 1741 (hex-waarde 06CD) te bekijken, **toont** de opdracht **ip-cachestroom | neem SrcIf|** _06_.*(01BB|06CD)_will weer geven de gerelateerde TCP NetFlow records zoals hier getoond:

TCP-stromen

```
router#show ip cache flow | include SrcIf|_06_.*(01BB|06CD)_
SrcIf          SrcIPaddress     DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0          192.168.18.79    Gi0/1          192.168.60.105  06 1C16 06CD     4
Gi0/0          192.168.101.251  Gi0/1          192.168.60.103  06 3A89 01BB     1
Gi0/0          192.168.40.131   Gi0/1          192.168.60.80   06 22FC 01BB     7
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 pakketten op de standaardpoorten, TCP-poort 443 en TCP-poort 1741, die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 is de IP adresruimte die door de beïnvloede apparaten wordt gebruikt, en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend.

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

```
! !-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable ports ! access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq https access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 1741 ! !-- 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
https access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq
1741 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !--
with existing security policies and configurations ! !-- Explicit deny for all other
IP traffic ! access-list tACL-Policy extended deny ip any any ! !-- Apply tACL to
```

```
interface(s) in the ingress direction ! access-group tACL-Policy in interface outside
```

Identificatie: Toegangscontrolelijsten voor douanevervoer

Nadat tACL is toegepast op een interface, kunnen beheerders de **show access-list** opdracht gebruiken om het aantal pakketten op TCP poort 443 en TCP poort 1741 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; 5 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq https (hitcnt=0)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 1741 (hitcnt=0)
access-list tACL-Policy line 3 extended deny tcp any 192.168.60.0 255.255.255.0 eq
https (hitcnt=15)
access-list tACL-Policy line 4 extended deny tcp any 192.168.60.0 255.255.255.0 eq
1741 (hitcnt=7)
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=0)
```

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

- **15** pakketten op **TCP-poort 443** voor ACE-lijn 3
- **7** pakketten op **TCP-poort 1741** voor ACE-lijn 4

Identificatie: berichten in Firewall Access List System

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

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

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

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

```
firewall#show logging | grep 106023
  Oct 21 2010 00:07:23: %ASA-4-106023: Deny tcp src outside:192.0.2.101/3710
         dst inside:192.168.60.112/1741 by access-group "tACL-Policy"
  Oct 21 2010 00:07:24: %ASA-4-106023: Deny tcp src outside:192.0.2.98/3711
```

```
        dst inside:192.168.60.27/443 by access-group "tACL-Policy"
  Oct 21 2010 00:07:24: %ASA-4-106023: Deny tcp src outside:192.0.2.149/3712
        dst inside:192.168.60.48/1741 by access-group "tACL-Policy"
  Oct 21 2010 00:07:24: %ASA-4-106023: Deny tcp src outside:192.0.2.172/3713
        dst inside:192.168.60.131/1741 by access-group "tACL-Policy"
  Oct 21 2010 00:07:24: %ASA-4-106023: Deny tcp src outside:192.0.2.129/3714
        dst inside:192.168.60.231/443 by access-group "tACL-Policy"
firewall#
```

In het voorafgaande voorbeeld, tonen de berichten die voor tACL *tACL-Policy* zijn geregistreerd pakketten voor **TCP-poort 443** en **TCP-poort 1741** die naar het adresblok zijn verzonden 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.

Cisco-inbraakpreventiesysteem

Beperken: acties voor Cisco IPS-handtekeningen

Beheerders kunnen Cisco Inbraakpreventiesysteem (IPS) gebruiken om bedreigingsdetectie te bieden en pogingen te voorkomen om de kwetsbaarheid te exploiteren die in dit document wordt beschreven. Beginnend met handtekeningsupdate S524 voor sensoren met Cisco IPS versie 6.x en hoger, kan de kwetsbaarheid worden gedetecteerd door handtekening 30859/0 (Handtekeningnaam: CiscoWorks Common Services Arbitary Code Execution Vulnerability). Handtekening 30859/0 is standaard ingeschakeld, activeert een gebeurtenis met *hoge* ernst, heeft een SFR (Signature Fidelity Rating) van 85 en is geconfigureerd met een **waarschuwing voor** standaardgebeurtenissen.

Vuren van handtekening 30859/0 wanneer één pakket wordt verzonden met behulp van TCP-poort 1741 gedetecteerd. Het afvuren van deze handtekening kan wijzen op een mogelijk misbruik van de kwetsbaarheid.

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

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

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

Cisco-systeem voor beveiligingsbewaking, analyse en respons

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

Het apparaat Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) kan incidenten veroorzaken met betrekking tot gebeurtenissen die verband houden met de kwetsbaarheid die in dit document wordt beschreven met behulp van IPS-handtekeningen 30859/0 (Handtekeningnaam: CiscoWorks Common Services Arbitary Code Execution Vulnerability). Nadat de dynamische handtekeningupdate S524 is gedownload, zal het gebruik van sleutelwoord **NR-30859/0** voor IPS handtekening 30859/0 en een vraagtype van **Alle overeenkomende gebeurtenissen** op Cisco Security MARS applicatie een rapport leveren dat een lijst maakt van de incidenten die door de IPS handtekening zijn gemaakt.

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

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

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

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

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

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

Aanvullende informatie

Revisiegeschiedenis

Revisie 1.0	2010-27 oktober	Eerste openbare

		publicatie

Cisco-beveiligingsprocedures

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

Gerelateerde informatie

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

Over deze vertaling

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