Identificatie en beperking van de benutting van de standaardreferenties voor basisaccount op de Cisco Media Experience Engine 5600

Identificatie en beperking van de benutting van de standaardreferenties voor basisaccount op de Cisco Media Experience Engine 5600

Advies-ID: cisco-amb-20110601-mxe

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110601-mxe

Revisie 1.0

Openbare publicatie 2011 juni 1 16:00 GMT

Inhoud

Cisco Response

Dit Toegepaste Matiging Bulletin is een begeleidend document aan de PSIRT Security Advisory *Default Credentials voor basisaccount op de Cisco Media Experience Engine 5600* en biedt identificatie- en mitigatietechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

Cisco Media Experience Engine (MXE) 5600 bevat een *root*-beheerdersaccount die standaard is ingeschakeld met een standaardwachtwoord. Deze kwetsbaarheid kan op afstand worden benut zonder authenticatie en zonder interactie van de eindgebruiker. Succesvolle exploitatie van deze kwetsbaarheid kan willekeurige code uitvoering toestaan of informatie openbaarmaking toestaan, die een aanvaller in staat stelt om informatie over het getroffen apparaat te leren. De aanvalsvector voor exploitatie is via SSH-pakketten met TCP-poort 2 en Telnet-pakketten met TCP-poort 23. Opmerking: Telnet is standaard uitgeschakeld op de Cisco MXE 5600, maar kan

worden gebruikt als een vector van exploitatie als het handmatig is ingeschakeld op getroffen apparaten.

Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-1623.

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-20110601-mxe.

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 infrastructuurtoegangscontrolelijsten (iACL's). Dit beschermingsmechanisme filtert en laat pakketten vallen die proberen deze kwetsbaarheid te exploiteren.

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

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

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

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

Risicobeheer

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

Apparaatspecifieke beperking en identificatie

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

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

- Cisco IOS-routers en -Switches
- Cisco IOS NetFlow
- Cisco ASA- en FWSM-firewalls

Cisco IOS-routers en -Switches

Beperking: toegangscontrolelijsten voor infrastructuur

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

Het iACL-beleid ontkent onbevoegde SSH-pakketten op TCP-poort 22 en Telnet-pakketten op TCP-poort 23 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. 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 22
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 23 ! !-- 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 22 deny tcp any 192.168.60.0
0.0.0.255 eq 23 ! !-- Explicit deny ACE for traffic sent to addresses configured
within !-- the infrastructure address space ! deny ip any 192.168.60.0 0.0.0.255 ! !-
- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-- with
existing security policies and configurations ! !-- Apply iACL to interfaces in the
ingress direction ! interface GigabitEthernet0/0 ip access-group Infrastructure-ACL-
Policy in
```

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

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

Identificatie: Toegangscontrolelijsten voor infrastructuur

Nadat de beheerder iACL op een interface heeft toegepast, zal de opdracht **IP-toegangslijsten tonen** het aantal SSH-pakketten op TCP-poort 22 en Telnet-pakketten op TCP-poort 23 identificeren die zijn gefilterd op interfaces waarop iACL is toegepast. De beheerders zouden gefilterde pakketten moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont ip toegang-lijsten** 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 ssh
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq telnet
    30 deny tcp any 192.168.60.0 0.0.0.255 eq ssh (23 matches)
    40 deny tcp any 192.168.60.0 0.0.0.255 eq telnet (17 matches)
    50 deny ip any 192.168.60.0 0.0.0.255
router#
```

In het vorige voorbeeld is de toegangslijst Infrastructuur-ACL-beleid 23 SSH-pakketten gedaald op TCP-poort 22 voor toegangscontrolelijst entry (ACE) lijn 30 en 17 Telnet-pakketten op **TCP**-poort **23** 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.

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 (2409 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .349 .650 .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
  89 active, 4007 inactive, 318 added
```

```
  4544 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             38      0.0         9    40      0.0       0.0      15.2
TCP-other          108      0.0         6    40      0.0       0.0      15.5
UDP-TFTP            10      0.0         4    28      0.0       0.0      15.7

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
UDP-other           73      0.0         7    28      0.0       0.0      15.5
Total:             229      0.0         7    35      0.0       0.0      15.5

SrcIf         SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.74.110  Et0/1          192.168.13.20   06 C8A7 D4BE     5
Et0/0         192.168.23.20   Et0/1          192.168.226.172 11 2123 540A     1
Et0/0         192.168.53.205  Et0/1          192.168.60.88   11 DEB7 0045     5
Et0/0         192.168.0.115   Et0/1          192.168.60.214  06 F73A 0050    11
Et0/0         192.168.0.30    Et0/1          192.168.60.63   06 A64E 0016     3
Et0/0         192.168.211.52  Et0/1          192.168.113.252 11 17AA 8F11    17
Et0/0         192.168.34.222  Et0/1          192.168.58.190  11 9A8F 2AD3     5
Et0/0         192.168.198.3   Et0/1          192.168.60.104  11 4F4D 0045     1
Et0/0         192.168.240.90  Et0/1          192.168.88.197  06 3D88 0017    15
Et0/0         192.168.0.96    Et0/1          192.168.60.126  06 9621 0017     3
Et0/0         192.168.155.22  Et0/1          192.168.80.13   06 1298 EB6A    10
Et0/0         192.168.0.20    Et0/1          192.168.60.78   06 1541 0050     3
Et0/0         192.168.0.2     Et0/1          192.168.60.195  06 5419 01BB     5
Et0/0         192.168.223.127 Et0/1          192.168.121.153 06 0613 17E5     7
Et0/0         192.168.0.28    Et0/1          192.168.60.101  06 B5C6 0017     2
Et0/0         192.168.92.207  Et0/1          192.168.43.167  11 1FF5 2815    11
Et0/0         192.168.0.28    Et0/1          192.168.60.139  06 24E9 0050     6
Et0/0         192.168.122.182 Et0/1          192.168.68.21   11 71C2 80BB    11
Et0/0         192.168.18.228  Et0/1          192.168.203.86  11 0630 77B4    16
Et0/0         192.168.0.218   Et0/1          192.168.60.248  06 531B 01BB    15
Et0/0         192.168.26.81   Et0/1          192.168.213.193 06 76D9 11B0     3
Et0/0         192.168.225.144 Et0/1          192.168.28.79   11 FF8F 299D    32
Et0/0         192.168.166.100 Et0/1          192.168.60.217  11 0B47 0045    10
Et0/0         192.168.49.15   Et0/1          192.168.139.203 11 D880 6D41     4
Et0/0         192.168.0.120   Et0/1          192.168.60.41   06 D24F 0016     6
Et0/0         192.168.0.109   Et0/1          192.168.60.189  06 B0B0 0016    11
Et0/0         192.168.0.65    Et0/1          192.168.60.136  06 6110 01BB     2
Et0/0         192.168.0.51    Et0/1          192.168.60.43   06 4090 0050    17
Et0/0         192.168.160.238 Et0/1          192.168.38.104  06 F54E DEE1    14
router#
```

In het bovenstaande voorbeeld zijn er meerdere stromen voor SSH op TCP poort 22 (hex waarde 0016) en **Telnet** op **TCP** poort **23 (hex waarde 0017)**.

Om alleen de verkeersstromen voor SSH-pakketten op TCP-poort 22 (hex-waarde 0016) en Telnet-pakketten op TCP-poort 23 (hex-waarde 0017) weer te geven, **toont** de opdracht **ip-cachestroom | inclusief SrcIf|**_06_.*0016|0017 zal de verwante TCP NetFlow-records weergeven zoals hier wordt getoond:

TCP-stromen

```
router#show ip cache flow | include SrcIf|_06_.*0016|0017
SrcIf         SrcIPaddress     DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.0.30     Et0/1          192.168.60.63   06 A64E 0016     3
Et0/0         192.168.0.120    Et0/1          192.168.60.41   06 D24F 0017     6
Et0/0         192.168.0.109    Et0/1          192.168.60.189  06 B0B0 0016    11
router#
```

Cisco ASA- en FWSM-firewalls

Beperking: toegangscontrolelijsten voor douanevervoer

Om het netwerk te beschermen tegen verkeer dat het netwerk ingaat op toegangspunten die internetverbindingspunten, partner- en leveranciersverbindingen 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 SSH-pakketten op TCP-poort 22 en Telnet-pakketten op TCP-poort 23 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 22 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 23 ! !-- 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
22 access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 23 !
!-- 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 SSH-pakketten op TCP-poort 22 en Telnet-pakketten op TCP-poort 23 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 ssh (hitcnt=485)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
  192.168.60.0 255.255.255.0 eq telnet (hitcnt=29)
access-list tACL-Policy line 3 extended deny tcp any
  192.168.60.0 255.255.255.0 eq ssh (hitcnt=58)
access-list tACL-Policy line 4 extended deny tcp any
  192.168.60.0 255.255.255.0 eq telnet (hitcnt=16)
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=8)
firewall#
```

In het voorafgaande voorbeeld, heeft de toegangslijst van ACL-Policy **58 SSH-**pakketten laten vallen op **TCP-poort 22** en **16 Telnet-**pakketten op **TCP-poort 23** die van een onbetrouwbare host of netwerk zijn ontvangen. Daarnaast kan syslog-bericht *106023* waardevolle informatie leveren, waaronder het IP-adres van de bron en de bestemming, de bron- en doelpoortnummers en het IP-protocol voor het ontkende pakket.

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
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.194/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.164/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.106/23 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.241/23 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.169/1025
 dst inside:192.168.60.56/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.36/1025
 dst inside:192.168.60.202/22 by access-group "tACL-Policy"
firewall#
```

In het voorafgaande voorbeeld, tonen de berichten die voor tACL tACL-Policy zijn geregistreerd **SSH-**pakketten voor **TCP-poort 22** en **Telnet-**pakketten voor **TCP-poort 23** verzonden naar het adresblok dat aan de infrastructuurapparaten is toegewezen.

Aanvullende informatie over syslogberichten voor ASA-beveiligingsapparaten is te vinden in

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

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

Aanvullende informatie

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

Revisiegeschiedenis

Revisie 1.0	2011-juni-01	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
- Identificatie en beperking van TTL-aanval bij verlopen
- Een security georiënteerde benadering van IP-adressering
- Tegenmaatregelen voor kwaadwillig gebruik van IPv6 Type 0-routingkoppen
- Opdrachttaal voor gereedschap beveiligen op Cisco IOS
- Cisco Firewallproducten - startpagina op Cisco.com
- 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.