

Identificatie en beperking van de exploitatie van Cisco IOS-software - Smart Install Remote Code - kwetsbaarheid

Identificatie en beperking van de exploitatie van Cisco IOS-software - Smart Install Remote Code - kwetsbaarheid

Advies-ID: cisco-amb-20110928-smart-install

<https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110928-smart-install>

Revisie 1.0

2011 september 28 00:00 UTC (GMT)

Inhoud

[Cisco Response](#)

[Apparaatspecifieke beperking en identificatie](#)

[Aanvullende informatie](#)

[Revisiegeschiedenis](#)

[Cisco-beveiligingsprocedures](#)

[Gerelateerde informatie](#)

Cisco Response

Dit Toegepaste Beperking Bulletin is een begeleidend document aan de PSIRT Security Advisory *Cisco IOS-software Smart Install Remote Code Execution Vulnerability* en biedt identificatie- en onderdrukkingstechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

Kwetsbaarheid Kenmerken

De functie Smart Install in Cisco Catalyst-Switches waarop Cisco IOS-software wordt uitgevoerd, bevat een kwetsbaarheid waarmee een externe aanvaller code op afstand kan uitvoeren op het betreffende apparaat. Deze kwetsbaarheid kan op afstand worden benut zonder authenticatie en zonder interactie van de eindgebruiker. De aanvalsvector voor exploitatie is via bewerkte Smart Install-pakketten met TCP-poort 4786.

Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-3271.

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory, die beschikbaar is via de volgende link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-smart-install>.

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

Risicobeheer

Organisaties wordt aangeraden om hun standaardprocessen voor risico-evaluatie en -beperking te volgen om de potentiële impact van [deze kwetsbaarheid|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 IOS-routers en -Switches

Beperking: toegangscontrolelijsten voor infrastructuur

Om infrastructuurapparaten te beschermen en het risico, de impact en de effectiviteit van directe infrastructuraanvallen 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 infrastructuurapparaten 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 onbevoegde Smart Install-pakketten op TCP-poort 4786 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 port ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 4786
!!-- The following vulnerability-specific access control entry !-- (ACE) can aid in
identification of attacks ! deny tcp any 192.168.60.0 0.0.0.255 eq 4786 !!--
Explicit deny ACE for traffic sent to addresses configured within !-- the
infrastructure address space ! deny ip any 192.168.60.0 0.0.0.255 !!-- Permit or
deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing security
policies and configurations !!-- Apply iACL to interfaces in the ingress direction !
interface GigabitEthernet0/0 ip access-group Infrastructure-ACL-Policy in
```

Merk op dat het filteren met een 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 toepast, zal de **opdracht IP-toeganglijsten tonen** het aantal Smart Install-pakketten op TCP-poort 4786 identificeren die zijn gefilterd op interfaces waarop iACL wordt toegepast. De beheerders zouden gefilterde pakketten moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het

voorbeeld voor toont ip toegang-lijsten Infrastructuur-ACL-Beleid volgt:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
 10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 4786
 20 deny tcp any 192.168.60.0 0.0.0.255 eq 4786 (13 matches)
 30 deny ip any 192.168.60.0 0.0.0.255
router#
```

In het vorige voorbeeld is de toegangslijst *Infrastructuur-ACL-Beleid* gedaald met 13 Smart Install-pakketten op TCP-poort 4786 voor lijn 20 van de toegangscontrolelijst (ACE).

Voor extra informatie over het onderzoeken van incidenten met ACE-tellers en syslog-gebeurtenissen, raadpleegt u de white paper [Identifying Incidents Use Firewall en IOS Router Syslog Events](#) Applied Intelligence. Beheerders kunnen Embedded Event Manager gebruiken om instrumentatie te bieden wanneer aan specifieke voorwaarden is voldaan, zoals ACE-tellers. De Applied Intelligence white paper [Embedded Event Manager in een security context](#) biedt aanvullende informatie over hoe deze functie te gebruiken. Identificatie: Vastlegging toegangslijst De optie log en log-input toegangscontrolelijst (ACL) zorgt ervoor dat pakketten die overeenkomen met specifieke ACE's worden vastgelegd. De log-input optie 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 mogelijk pogingen zijn om deze kwetsbaarheid te exploiteren. Beheerders wordt aangeraden om stromen te onderzoeken om te bepalen of ze pogingen zijn om deze kwetsbaarheid te exploiteren of dat ze legitieme verkeersstromen zijn.

```
router#show ip cache flow
```

```
IP packet size distribution (90784136 total packets):
```

```

1-32  64  96  128  160  192  224  256  288  320  352  384  416  448  480
.000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

```

IP Flow Switching Cache, 4456704 bytes

```

1885 active, 63651 inactive, 59960004 added
129803821 aget polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds

```

IP Sub Flow Cache, 402056 bytes

```

0 active, 16384 inactive, 0 added, 0 added to flow
0 alloc failures, 0 force free
1 chunk, 1 chunk added
last clearing of statistics never

```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	11393421	2.8	1	48	3.1	0.0	1.4
TCP-FTP	236	0.0	12	66	0.0	1.8	4.8
TCP-FTPD	21	0.0	13726	1294	0.0	18.4	4.1
TCP-WWW	22282	0.0	21	1020	0.1	4.1	7.3
TCP-X	719	0.0	1	40	0.0	0.0	1.3
TCP-BGP	1	0.0	1	40	0.0	0.0	15.0
TCP-Frag	70399	0.0	1	688	0.0	0.0	22.7
TCP-other	47861004	11.8	1	211	18.9	0.0	1.3
UDP-DNS	582	0.0	4	73	0.0	3.4	15.4
UDP-NTP	287252	0.0	1	76	0.0	0.0	15.5
UDP-other	310347	0.0	2	230	0.1	0.6	15.9
ICMP	11674	0.0	3	61	0.0	19.8	15.5
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	4	0.0	1	48	0.0	0.0	15.3
Total:	59957957	14.8	1	196	22.5	0.0	1.5

```

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts

```

Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	06	0911	12B2	3
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016	12CA	1
Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	06	0B89	12B2	10
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B	007B	1

router#

In het bovenstaande voorbeeld zijn er meerdere stromen voor Smart Install-pakketten op TCP-poort 4786 (hex-waarde 0x12B2). Om alleen de verkeersstromen voor pakketten op TCP-poort 22 (hex-waarde 0x16) te bekijken, toont de opdracht ip-cachestroom | neem SrcIf|_06_.*12B2_ zal de verwante verslagen van TCP NetFlow zoals hier getoond tonen: TCP-stromen

```
router#show ip cache flow | include SrcIf|_06_.*0016
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	06	0911	12B2	3
Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	06	0B89	12B2	10

router#

[Cisco ASA- en FWSM-firewalls](#) Beperking: toegangscontrolelijsten voor douanevervoer Om het netwerk te beschermen tegen verkeer dat het netwerk ingaat op toegangspunten die internetverbindingpunten, partner- en leveranciersverbindingen of VPN-verbindingpunten 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 onbevoegde pakketten op TCP-poort 4786 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 de [Transit Access Control Lists: Filtering at Your Edge](#).

```
!!-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable port !! access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 4786 !!-- The following vulnerability-
specific access control entry !-- (ACE) can aid in identification of attack ! access-
list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 4786 !!--
```

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 Smart Install pakketten op TCP poort 4786 te identificeren die zijn gefilterd. De beheerders worden geadviseerd om gefilterde pakketten te onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor toont toegang-lijst aan ACL-Beleid volgt:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 3 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
    192.168.60.0 255.255.255.0 eq 4786
access-list tACL-Policy line 2 extended deny tcp any
    192.168.60.0 255.255.255.0 eq 4786 (hitcnt=80)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

In het vorige voorbeeld heeft toegangslijst *tACL-Policy* 80 Smart Install-pakketten gedaald op TCP-poort 4786 voor ACE-lijn 2. Identificatie: berichten in Firewall Access List

SystemFirewallsyslog-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 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 [Een reguliere expressie maken](#).

```
firewall#show logging | grep 106023
Feb 21 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
```

```
dst inside:192.168.60.240/4786 by access-group "tACL-Policy"
```

```
Feb 21 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
```

```
dst inside:192.168.60.38/4786 by access-group "tACL-Policy"
```

```
firewall#
```

In het vorige voorbeeld, tonen de berichten die voor tACL *tACL-Policy* worden geregistreerd pakketten voor TCP-poort 4786 die naar het adresblok worden verzonden dat aan getroffen apparaten wordt toegewezen. Aanvullende informatie over syslogberichten voor ASA-beveiligingsapparaten is te vinden in [Cisco ASA 5500 Series systeemlogberichten, 8.2](#).

Aanvullende informatie over syslog-berichten voor de FWSM is te vinden in [Catalyst 6500 Series Switch en Cisco 7600 Series router Firewall Services Module Logging System Berichten](#). Voor

extra informatie over het onderzoeken van incidenten met behulp van syslog-gebeurtenissen, raadpleegt u het white paper [Identifying Incidents Use Firewall en IOS Router Syslog Events](#)

Applied Intelligence. **Aanvullende informatie** DIT DOCUMENT WORDT AANGEBODEN OP EEN 'AS IS'-BASIS EN IMPLICEERT GEEN ENKEL SOORT GARANTIE, MET INBEGRIIP 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	2011-28 SEPTEMBER	Eerste openbare publicatie
-------------	-------------------	----------------------------

Cisco-beveiligingsprocedures Volledige informatie over het melden van beveiligingskwetsbaarheden in Cisco-producten, het verkrijgen van assistentie bij beveiligingsincidenten en het registreren om beveiligingsinformatie van Cisco te ontvangen, is beschikbaar op de wereldwijde website van Cisco op

https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Dit

omvat instructies voor persvragen over Cisco-beveiligingsmeldingen. Alle Cisco-

beveiligingsadviezen zijn beschikbaar op <http://www.cisco.com/go/psirt>.

Gerelateerde informatie

- [Cisco-bulletins voor toegepaste beperking](#)
- [Cisco-beveiligingsintelligentie](#)
- [Cisco Security IntelliShield Alert Manager-service](#)
- [Cisco-handleiding over het versterken van Cisco IOS-apparaten](#)
- [Cisco IOS NetFlow - startpagina op Cisco.com](#)

- [Cisco IOS NetFlow-witboeken](#)
- [NetFlow-prestatieanalyse](#)
- [Witboeken voor Cisco Network Foundation-bescherming](#)
- [Presentaties voor Cisco Network Foundation-bescherming](#)
- [Een security georiënteerde benadering van IP-adressering](#)
- [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.