Identificazione e mitigazione dello sfruttamento di più vulnerabilità DoS nei prodotti Cisco Unified Communications

Identificazione e mitigazione dello sfruttamento di più vulnerabilità DoS nei prodotti Cisco Unified Communications

ID advisory: cisco-amb-20100825-cucm-cup

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100825-cucm-cup

Revisione 1.0

Per la Pubblica Release 2010 Agosto 25 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Il presente Bollettino sulla mitigazione applicata è un documento complementare ai consigli sulla sicurezza PSIRT, alle vulnerabilità Denial of Service di Cisco Unified Communications Manager e alle vulnerabilità Cisco Unified Presence Denial of Service e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

Il processo SIP dei prodotti Cisco Unified Communications Manager e Cisco Unified Presence presenta diverse vulnerabilità. Le seguenti sottosezioni riepilogano queste vulnerabilità:

Vulnerabilità Denial of Service (DoS) di Cisco Unified Communications Manager: queste vulnerabilità possono essere sfruttate in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di queste vulnerabilità può determinare una condizione DoS (Denial of Service). I ripetuti tentativi di sfruttare queste vulnerabilità potrebbero generare una

condizione DoS prolungata.

I vettori di attacco per l'utilizzo sono attraverso pacchetti SIP che utilizzano i seguenti protocolli e porte:

- SIP con porta TCP 5060
- SIP con porta TCP 5061
- SIP con porta UDP 5060
- SIP con porta UDP 5061

Un utente non autorizzato potrebbe sfruttare queste vulnerabilità utilizzando pacchetti di spoofing.

A queste vulnerabilità sono stati assegnati gli identificatori CVE CVE-2010-2837 e CVE-2010-2838.

Vulnerabilità Cisco Unified Presence Denial of Service (DoS): queste vulnerabilità possono essere sfruttate in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di queste vulnerabilità può determinare una condizione DoS (Denial of Service). I ripetuti tentativi di sfruttare queste vulnerabilità potrebbero generare una condizione DoS prolungata.

I vettori di attacco per l'utilizzo sono attraverso pacchetti SIP che utilizzano i seguenti protocolli e porte:

- SIP con porta TCP 5060
- SIP con porta TCP 5061
- SIP con porta UDP 5060
- SIP con porta UDP 5061

Un utente non autorizzato potrebbe sfruttare queste vulnerabilità utilizzando pacchetti di spoofing.

A queste vulnerabilità sono stati assegnati gli identificatori CVE CVE-2010-2839 e CVE-2010-2840.

Le informazioni sul software vulnerabile, non interessato e fisso sono disponibili nei consigli per la sicurezza PSIRT, disponibili ai seguenti link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100825-cucm e https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100825-cup.

Panoramica delle tecniche di mitigazione

I dispositivi Cisco forniscono diverse contromisure per queste vulnerabilità. Si consiglia agli amministratori di considerare questi metodi di protezione come best practice generali per la sicurezza dei dispositivi dell'infrastruttura e del traffico che attraversa la rete. In questa sezione del documento viene fornita una panoramica di queste tecniche.

Il software Cisco IOS® è in grado di fornire mezzi efficaci di prevenzione degli attacchi tramite i seguenti metodi:

- Access Control List (tACL) transit
- Inoltro percorso inverso unicast (RPF unicast)

- IPSG (IP Source Guard)

Questi meccanismi di protezione filtrano e rilasciano, oltre a verificare l'indirizzo IP di origine dei pacchetti che stanno tentando di sfruttare queste vulnerabilità.

L'installazione e la configurazione corrette di RPF unicast offrono un mezzo efficace di protezione dagli attacchi che utilizzano pacchetti con indirizzi IP di origine oggetto di spoofing. È consigliabile distribuire RPF unicast il più vicino possibile a tutte le origini di traffico.

La corretta installazione e configurazione di IPSG fornisce un mezzo efficace di protezione dagli attacchi di spoofing a livello di accesso.

Mezzi efficaci per prevenire gli attacchi possono essere forniti anche da Cisco ASA serie 5500 Adaptive Security Appliance e dal Firewall Services Module (FWSM) per Cisco Catalyst 6500.

- tACL
- RPF unicast

Questi meccanismi di protezione filtrano e rilasciano, oltre a verificare l'indirizzo IP di origine dei pacchetti che stanno tentando di sfruttare queste vulnerabilità.

L'uso efficace delle azioni evento di Cisco Intrusion Prevention System (IPS) offre visibilità e protezione dagli attacchi che tentano di sfruttare queste vulnerabilità.

I record Cisco IOS NetFlow possono fornire visibilità sui tentativi di sfruttamento basati sulla rete.

I firewall del software Cisco IOS, Cisco ASA e FWSM possono fornire visibilità attraverso i messaggi syslog e i valori dei contatori visualizzati nell'output dei comandi **show**.

L'accessorio Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) può inoltre fornire visibilità attraverso richieste, segnalazioni di incidenti e query.

Gestione dei rischi

Le organizzazioni sono invitate a seguire i processi standard di valutazione e mitigazione dei rischi per determinare l'impatto potenziale di queste vulnerabilità. Triage si riferisce all'ordinamento dei progetti e all'assegnazione delle priorità agli sforzi che hanno maggiori probabilità di avere successo. Cisco ha fornito documenti che possono aiutare le organizzazioni a sviluppare una funzionalità di triage basata sui rischi per i team addetti alla sicurezza delle informazioni. Valutazione dei rischi per la vulnerabilità della sicurezza Gli annunci e la valutazione dei rischi e la creazione di prototipi possono aiutare le organizzazioni a sviluppare processi ripetibili di valutazione della sicurezza e di risposta.

Mitigazione e identificazione specifiche del dispositivo

Attenzione: l'efficacia di qualsiasi tecnica di mitigazione dipende dalle situazioni specifiche del cliente, come il mix di prodotti, la topologia di rete, il comportamento del traffico e la missione organizzativa. Come per qualsiasi modifica apportata alla configurazione, valutare l'impatto della configurazione prima di applicare la modifica.

Per questi dispositivi sono disponibili informazioni specifiche sulla mitigazione e l'identificazione:

- Router e switch Cisco IOS

- Cisco IOS NetFlow
- Cisco ASA e firewall FWSM
- Cisco Intrusion Prevention System
- Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco

Router e switch Cisco IOS

Attenuazione: Access Control List transit

Per proteggere la rete dal traffico che entra nei punti di accesso in entrata, che possono includere punti di connessione Internet, punti di connessione fornitori e partner o punti di connessione VPN, si consiglia agli amministratori di distribuire elenchi di controllo di accesso in transito (tACL) per applicare le policy. Gli amministratori possono costruire un ACL autorizzando esplicitamente solo il traffico autorizzato ad accedere alla rete dai punti di accesso in entrata o autorizzando il traffico autorizzato a transitare sulla rete in base alle configurazioni e ai criteri di sicurezza esistenti. Una soluzione ACL non può fornire una protezione completa da queste vulnerabilità quando l'attacco ha origine da un indirizzo di origine attendibile.

Il criterio ACL nega l'invio ai dispositivi interessati di pacchetti SIP non autorizzati sulle porte TCP 5060 e 5061 e sulle porte UDP 5060 e 5061. Nell'esempio seguente, 192.168.60.0/24 è lo spazio di indirizzi IP utilizzato dai dispositivi interessati e l'host con indirizzo 192.168.100.1 è considerato una fonte attendibile che richiede l'accesso ai dispositivi interessati. È necessario prestare attenzione a consentire il traffico richiesto per il routing e l'accesso amministrativo prima di rifiutare tutto il traffico non autorizzato.

Per ulteriori informazioni sugli ACL, consultare il documento Access Control Lists: Filtering at Your Edge (Liste di controllo dell'accesso in transito: filtraggio sul perimetro della rete).

```
!-- 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 5060 access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5061 access-list 150 permit udp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5060 access-list 150 permit udp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 5061 ! !-- 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 5060 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq
5061 access-list 150 deny udp any 192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny
udp any 192.168.60.0 0.0.0.255 eq 5061 ! !-- 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
```

L'applicazione di un filtro con un elenco degli accessi all'interfaccia determinerà la trasmissione di messaggi ICMP "destinazione irraggiungibile" alla sorgente del traffico filtrato. La generazione di questi messaggi potrebbe avere l'effetto indesiderato di aumentare l'utilizzo della CPU sul dispositivo. Per impostazione predefinita, nel software Cisco IOS la generazione di pacchetti ICMP "destinazione irraggiungibile" è limitata a un pacchetto ogni 500 millisecondi. La generazione di messaggi ICMP "destinazione irraggiungibile" può essere disabilitata usando il comando di configurazione interfaccia **no ip unreachables**. La limitazione della velocità non raggiungibile ICMP può essere modificata dal valore predefinito utilizzando il comando di configurazione globale **ip**

icmp rate-limit unreachable *interval-in-ms*.

Attenuazione: protezione da spoofing

Inoltro percorso inverso unicast

Le vulnerabilità descritte in questo documento possono essere sfruttate da pacchetti IP oggetto di spoofing. Gli amministratori possono distribuire e configurare Unicast Reverse Path Forwarding (Unicast RPF) come meccanismo di protezione contro lo spoofing.

Unicast RPF è configurato a livello di interfaccia ed è in grado di rilevare ed eliminare pacchetti privi di un indirizzo IP di origine verificabile. Per garantire una protezione completa da spoofing, gli amministratori non devono fare affidamento su RPF unicast, in quanto i pacchetti oggetto di spoofing possono entrare nella rete tramite un'interfaccia abilitata per RPF unicast se esiste una route di ritorno appropriata all'indirizzo IP di origine. È consigliabile che gli amministratori verifichino che durante la distribuzione di questa funzionalità sia configurata la modalità RPF unicast appropriata (libera o rigida), in quanto può causare la perdita di traffico legittimo in transito sulla rete. In un ambiente aziendale, è possibile abilitare RPF unicast sul perimetro Internet e sul livello di accesso interno sulle interfacce di layer 3 supportate dall'utente.

Per ulteriori informazioni, consultare la guida alla funzionalità di inoltro percorso inverso unicast in modalità alloose.

Per ulteriori informazioni sulla configurazione e l'utilizzo di RPF unicast, consultare il white paper Understanding Unicast Reverse Path Forwarding Applied Intelligence.

Protezione origine IP

IPSG (IP Source Guard) è una funzione di sicurezza che limita il traffico IP su interfacce di livello 2 non instradate filtrando i pacchetti in base al database di binding dello snooping DHCP e ai binding di origine IP configurati manualmente. Gli amministratori possono utilizzare il protocollo IPSG per prevenire gli attacchi degli utenti non autorizzati che tentano di falsificare i pacchetti falsificando l'indirizzo IP di origine e/o l'indirizzo MAC. Se correttamente implementato e configurato, IPSG, insieme a RPF unicast in modalità rigorosa, fornisce i mezzi più efficaci per la protezione da spoofing delle vulnerabilità descritte in questo documento.

Per ulteriori informazioni sulla distribuzione e la configurazione di IPSG, consultare il documento sulla configurazione delle funzionalità DHCP e di IP Source Guard.

Identificazione: Access Control List transit

Dopo che l'amministratore ha applicato l'ACL a un'interfaccia, il comando **show ip access-lists** restituisce il numero di pacchetti SIP sulle porte TCP 5060 e 5061 e sulle porte UDP 5060 e 5061 filtrati. Gli amministratori sono invitati a indagare sui pacchetti filtrati per determinare se sono tentativi di sfruttare queste vulnerabilità. Di seguito è riportato un esempio di output per **show ip access-lists 150**:

```
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 5060 (1 match)
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 (31 matches)
    30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060 (15 matches)
    40 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061 (5 matches)
```

```
50 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (227 matches)
60 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (257 matches)
70 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (130 matches)
80 deny udp any 192.168.60.0 0.0.0.255 eq 5061 (175 matches)
90 deny ip any any (5219 matches)
```

Nell'esempio precedente, l'elenco degli accessi 150 ha eliminato i seguenti pacchetti provenienti da un host o da una rete non attendibile:

- **227** pacchetti **SIP** sulla **porta TCP 5060** per la linea ACE 50
- **257** pacchetti **SIP** sulla **porta TCP 5061** per la linea ACE 60
- **130** pacchetti **SIP** sulla **porta UDP 5060** per ACE line 70
- **175** pacchetti **SIP** sulla **porta UDP 5061** per la linea ACE 80

Per ulteriori informazioni sull'analisi degli incidenti tramite i contatori ACE e gli eventi syslog, consultare il white paper sull'identificazione degli incidenti tramite il firewall e gli eventi syslog del router IOS Application Intelligence.

Gli amministratori possono utilizzare Embedded Event Manager per fornire strumentazione quando vengono soddisfatte condizioni specifiche, ad esempio accessi al contatore ACE. Il white paper sull'intelligence applicata Embedded Event Manager in a Security Context fornisce ulteriori dettagli sull'utilizzo di questa funzionalità.

Identificazione: Registrazione elenco accessi

L'opzione **log** e **log-input** access control list (ACL) causerà la registrazione dei pacchetti che corrispondono ad ACE specifici. L'opzione **log-input** abilita la registrazione dell'interfaccia in entrata, oltre agli indirizzi IP di origine e destinazione dei pacchetti e alle porte.

Attenzione: la registrazione delle liste di controllo degli accessi può richiedere un utilizzo intensivo della CPU e deve essere utilizzata con estrema cautela. I fattori che determinano l'impatto della registrazione ACL sulla CPU sono la generazione di log, la trasmissione di log e la commutazione di processo per inoltrare i pacchetti che corrispondono alle voci ACE abilitate per il log.

Per il software Cisco IOS, il comando **ip access-list logging interval** *in-ms* può limitare gli effetti della commutazione di processo indotta dalla registrazione ACL. Il comando **logging rate-limit** *rate-per-second* [**except** *loglevel*] limita l'impatto della generazione e della trasmissione del log.

L'impatto sulla CPU causato dalla registrazione degli ACL può essere risolto tramite hardware sugli switch Cisco Catalyst serie 6500 e sui router Cisco serie 7600 con Supervisor Engine 720 o Supervisor Engine 32 utilizzando la registrazione degli ACL ottimizzata.

Per ulteriori informazioni sulla configurazione e l'utilizzo della registrazione ACL, consultare il white paper Understanding Access Control List Logging Applied Intelligence.

Identificazione: protezione da spoofing con inoltro percorso inverso unicast

Se il protocollo RPF unicast è installato e configurato correttamente nell'infrastruttura di rete, gli amministratori possono utilizzare i *comandi* show cef *type slot/port internal*, show ip interface, **show cef drop**, **show ip cef switching statistics** e **show ip traffic** per identificare il numero di pacchetti scartati dal protocollo RPF unicast.

Nota: a partire dal software Cisco IOS versione 12.4(20)T, il comando **show ip cef switching** è stato sostituito da **show ip cef switching statistics feature**.

Nota: il *comando* **show** | **begin** *regex* and **show**, *comando* | **include** *regex* i modificatori di comando vengono utilizzati negli esempi seguenti per ridurre al minimo la quantità di output che gli amministratori dovranno analizzare per visualizzare le informazioni desiderate. Per ulteriori informazioni sui modificatori di comandi, consultare le sezioni show command della guida di riferimento dei comandi di 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#
```

Nota: **show cef interface** *type slot/port* **internal è un comando nascosto che deve essere immesso completamente nell'interfaccia della riga di comando.** Il completamento del comando non è disponibile.

```
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#
```

Nelle versioni precedenti, **show cef drop**, **show ip cef switching statistics feature** e **show ip traffic** example, Unicast RPF ha scartato **18 pacchetti IP** ricevuti a livello globale su tutte le interfacce con RPF unicast configurato a causa dell'impossibilità di verificare l'indirizzo di origine dei pacchetti IP nella base di informazioni sull'inoltro di Cisco Express Forwarding.

Cisco IOS NetFlow

Identificazione: Identificazione del flusso di traffico mediante i record NetFlow

Gli amministratori possono configurare Cisco IOS NetFlow sui router e gli switch Cisco IOS per aiutare a identificare i flussi di traffico che potrebbero essere tentativi di sfruttare queste vulnerabilità. Si consiglia agli amministratori di analizzare i flussi per determinare se si tratta di tentativi di sfruttare queste vulnerabilità o se si tratta di flussi di traffico legittimi.

```
router#show ip cache flow
IP packet size distribution (54955 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .082 .531 .375 .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 .009 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  167 active, 3929 inactive, 32741 added
  607632 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            109      0.0         3    40      0.0       0.0      15.4
TCP-BGP          28425      0.0         1    68      0.0       2.9      15.4
TCP-other         1111      0.0         6    40      0.0       0.0      15.4
UDP-NTP           2221      0.0         1    76      0.0       0.0      15.6
UDP-TFTP            95      0.0         4    28      0.0       0.0      15.6
UDP-other          589      0.0         6    28      0.0       0.0      15.4
ICMP                24      0.0        31  1009      0.0      19.9      15.4
Total:           32574      0.0         1    75      0.0       2.5      15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.68.44   Et0/1         192.168.60.212  06 F208 098B     4
Et0/0         192.168.38.121  Et0/1         192.168.60.6    06 A826 01BB     3
Et0/0         192.168.224.241 Et0/1         192.168.60.182  06 7536 13C5     5
Et0/0         192.168.212.211 Et0/1         192.168.60.114  06 AB5E 01BB     2
Et0/0         192.168.205.69  Et0/1         192.168.60.110  06 98A5 0ABC    10
Et0/0         192.168.40.45   Et0/1         192.168.60.42   06 5FA7 01BB     2
Et0/0         192.168.4.192   Et0/1         192.168.93.248  11 FFFE 8002    15
Et0/0         192.168.44.66   Et0/1         192.168.178.29  06 A30D 0F4A     3
Et0/0         192.168.36.239  Et0/1         192.168.60.214  11 BCA3 0045     3
Et0/0         192.168.60.164  Et0/1         192.168.60.26   11 1EFB 13C4     2
Et0/0         192.168.234.206 Et0/1         192.168.147.20  11 C959 9972    17
Et0/0         192.168.148.143 Et0/1         192.168.60.25   11 CD48 0045     2
Et0/0         192.168.250.187 Et0/1         192.168.60.41   06 C5B3 098B     3
Et0/0         192.168.227.167 Et0/1         192.168.125.75  06 1048 23FC     3
Et0/0         192.168.107.126 Et0/1         192.168.194.53  06 3767 139B    13
Et0/0         192.168.1.194   Et0/0         192.168.60.155  06 CE95 098B   192
Et0/0         192.168.118.14  Et0/1         192.168.226.46  11 3966 FF31     8
Et0/0         192.168.35.154  Et0/1         192.168.60.77   06 3C5C 0ABC     1
Et0/0         192.168.145.167 Et0/1         192.168.60.74   11 B06D 0045     7
Et0/0         192.168.56.109  Et0/1         192.168.247.33  11 3F4C 9E2C     6
Et0/0         192.168.28.223  Et0/1         192.168.60.154  06 B35D 13C4     1
Et0/0         192.168.139.201 Et0/1         192.168.60.229  06 8E56 07D0     2
Et0/0         192.168.60.199  Et0/1         192.168.60.242  11 37AF 13C4     5
Et0/0         192.168.212.244 Et0/1         192.168.59.244  06 9CB9 95F7    12
Et0/0         192.168.133.250 Et0/1         192.168.60.49   06 41A2 098B     4
Et0/0         192.168.92.118  Et0/1         192.168.13.136  11 82E2 95B8     2
Et0/0         192.168.206.122 Et0/1         192.168.54.12   06 A09B 7514    11
Et0/0         192.168.164.86  Et0/1         192.168.60.44   11 4ED8 0045     7
Et0/0         192.168.144.222 Et0/1         192.168.60.188  06 770C 13C4     1
Et0/0         192.168.138.85  Et0/1         192.168.60.38   11 9B7D 13C4    11
Et0/0         192.168.185.139 Et0/1         192.168.97.208  11 A25E FE8C     8
```

```
Et0/0         192.168.78.45   Et0/1          192.168.92.184  11 08B5 BD08    13
Et0/0         192.168.2.81    Et0/1          192.168.60.138  11 3258 13C5     2
Et0/0         192.168.144.96  Et0/1          192.168.99.50   06 9D6D 4E7E    15
router#
```

Nell'esempio precedente, sono presenti più flussi per il SIP sulle porte TCP (valore esadecimale del protocollo 06) 5060 (valore esadecimale 13C4) e 5061 (valore esadecimale 13C5) e UDP (valore esadecimale del protocollo 11) sulle porte **5060 (valore esadecimale 13C4)** e **5061 (valore esadecimale 13C5)**.

Parte di questo traffico ha origine e viene inviato agli indirizzi inclusi nel blocco di indirizzi 192.168.60.0/24, che viene utilizzato dai dispositivi interessati. I pacchetti in questi flussi possono essere oggetto di spoofing e possono indicare un tentativo di sfruttare queste vulnerabilità. Si consiglia agli amministratori di confrontare questi flussi con l'utilizzo di base per il traffico SIP inviato sulle porte TCP 5060 e 5061 e sulle porte UDP 5060 e 5061, nonché di esaminare i flussi per determinare se provengono da host o reti non attendibili.

Per visualizzare solo i flussi di traffico per i pacchetti SIP sulle porte TCP (valore esadecimale del protocollo 06), 5060 (valore esadecimale 13C4), 5061 (valore esadecimale 13C5) e UDP (valore esadecimale del protocollo 11), 5060 (valore esadecimale 13C4) e 5061 (valore esadecimale 13C5), i comandi **show ip cache flow | includere SrcIf**|*_06_.*(13C4|13C5)* e **visualizzare il flusso della cache IP | include SrcIf**|*_11_.*(13C4|13C5)* visualizzerà i record NetFlow TCP e UDP correlati, come mostrato di seguito:

Flussi TCP

```
router#show ip cache flow | include SrcIf|_06_.*(13C4|13C5)
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.114.191 Et0/1          192.168.60.53   06 1713 13C4     4
Et0/0         192.168.40.246  Et0/1          192.168.60.145  06 CC2D 13C5     9
Et0/0         192.168.147.251 Et0/1          192.168.60.183  06 E2E1 13C4     1
Et0/0         192.168.88.150  Et0/1          192.168.60.197  06 6E1D 13C5    10
Et0/0         192.168.16.232  Et0/1          192.168.60.235  06 BD24 13C4     4
Et0/0         192.168.30.204  Et0/1          192.168.60.16   06 1A93 13C4     3
Et0/0         192.168.65.79   Et0/1          192.168.60.223  06 3FD5 13C5     2
Et0/0         192.168.82.123  Et0/1          192.168.60.100  06 ACA7 13C4     2
Et0/0         192.168.224.47  Et0/1          192.168.60.178  06 5BD7 13C4     3
Et0/0         192.168.87.54   Et0/1          192.168.60.49   06 D55B 13C5     2
router#
```

Flussi UDP

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.151.1   Et0/1          192.168.60.96   11 2C2D 13C5     3
Et0/0         192.168.237.123 Et0/1          192.168.60.131  11 5712 13C5     4
Et0/0         192.168.246.100 Et0/1          192.168.60.37   11 FCBC 13C5     4
Et0/0         192.168.126.21  Et0/1          192.168.60.103  11 9716 13C4     1
Et0/0         192.168.60.28   Et0/1          192.168.60.244  11 E40B 13C4   192
Et0/0         192.168.56.139  Et0/1          192.168.60.218  11 4EE8 13C4    10
Et0/0         192.168.51.212  Et0/1          192.168.60.209  11 835D 13C4     3
Et0/0         192.168.252.73  Et0/1          192.168.60.115  11 521E 13C4     3
router#
```

Cisco ASA e firewall FWSM

Attenuazione: Access Control List transit

Per proteggere la rete dal traffico che entra nei punti di accesso in entrata, che possono includere punti di connessione Internet, punti di connessione fornitori e partner o punti di connessione VPN, si consiglia agli amministratori di distribuire gli ACL per applicare la policy. Gli amministratori possono costruire un ACL autorizzando esplicitamente solo il traffico autorizzato ad accedere alla rete dai punti di accesso in entrata o autorizzando il traffico autorizzato a transitare sulla rete in base alle configurazioni e ai criteri di sicurezza esistenti. Una soluzione ACL non può fornire una protezione completa da queste vulnerabilità quando l'attacco ha origine da un indirizzo di origine attendibile.

Il criterio ACL nega l'invio ai dispositivi interessati di pacchetti SIP non autorizzati sulle porte TCP 5060 e 5061 e sulle porte UDP 5060 e 5061. Nell'esempio seguente, 192.168.60.0/24 è lo spazio di indirizzi IP utilizzato dai dispositivi interessati e l'host con indirizzo 192.168.100.1 è considerato una fonte attendibile che richiede l'accesso ai dispositivi interessati. È necessario prestare attenzione a consentire il traffico richiesto per il routing e l'accesso amministrativo prima di rifiutare tutto il traffico non autorizzato.

Per ulteriori informazioni sugli ACL, consultare il documento Access Control Lists: Filtering at Your Edge (Liste di controllo dell'accesso in transito: filtraggio sul perimetro della rete).

```
! !-- 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 5060 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-
Policy extended permit udp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5060
access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061 ! !-- 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 5060 access-list tACL-Policy
extended deny tcp any 192.168.60.0 255.255.255.0 eq 5061 access-list tACL-Policy
extended deny udp any 192.168.60.0 255.255.255.0 eq 5060 access-list tACL-Policy
extended deny udp any 192.168.60.0 255.255.255.0 eq 5061 ! !-- 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
```

Attenuazione: protezione da spoofing con inoltro percorso inverso unicast

Le vulnerabilità descritte in questo documento possono essere sfruttate da pacchetti IP oggetto di spoofing. Gli amministratori possono distribuire e configurare RPF unicast come meccanismo di protezione contro lo spoofing.

Unicast RPF è configurato a livello di interfaccia ed è in grado di rilevare ed eliminare pacchetti privi di un indirizzo IP di origine verificabile. Per garantire una protezione completa da spoofing, gli amministratori non devono fare affidamento su RPF unicast, in quanto i pacchetti oggetto di spoofing possono entrare nella rete tramite un'interfaccia abilitata per RPF unicast se esiste una route di ritorno appropriata all'indirizzo IP di origine. In un ambiente aziendale, è possibile abilitare RPF unicast sul perimetro Internet e sul livello di accesso interno sulle interfacce di layer 3 supportate dall'utente.

Per ulteriori informazioni sulla configurazione e l'utilizzo di RPF unicast, consultare la guida di riferimento dei comandi di Cisco Security Appliance per ip verify reverse-path e il white paper Understanding Unicast Reverse Path Forwarding Applied Intelligence.

Identificazione: Access Control List transit

Dopo aver applicato l'ACL a un'interfaccia, gli amministratori possono usare il comando **show access-list** per identificare il numero di pacchetti SIP sulle porte TCP 5060 e 5061 e sulle porte UDP 5060 e 5061 filtrati. Gli amministratori sono invitati a indagare sui pacchetti filtrati per determinare se sono tentativi di sfruttare queste vulnerabilità. Di seguito è riportato un output di esempio per **show access-list tACL-Policy**:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 9 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
               192.168.60.0 255.255.255.0 eq sip (hitcnt=224)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=28)
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1
               192.168.60.0 255.255.255.0 eq sip (hitcnt=36)
access-list tACL-Policy line 4 extended permit udp host 192.168.100.1
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=41)
access-list tACL-Policy line 5 extended deny tcp any
               192.168.60.0 255.255.255.0 eq sip (hitcnt=78)
access-list tACL-Policy line 6 extended deny tcp any
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=39)
access-list tACL-Policy line 7 extended deny udp any
               192.168.60.0 255.255.255.0 eq sip (hitcnt=437)
access-list tACL-Policy line 8 extended deny udp any
               192.168.60.0 255.255.255.0 eq 5061 (hitcnt=478)
access-list tACL-Policy line 9 extended deny ip any any (hitcnt=563)
firewall#
```

Nell'esempio precedente, *tACL-Policy dell'*elenco degli accessi ha eliminato i seguenti pacchetti ricevuti da un host o una rete non attendibile:

- **78** pacchetti **SIP** sulla **porta TCP 5060 (sip)** per la linea ACE 5
- **39** pacchetti **SIP** sulla **porta TCP 5061** per la linea ACE 6
- **437** pacchetti **SIP** sulla **porta UDP 5060 (sip)** per la linea ACE 7
- **478** pacchetti **SIP** sulla **porta UDP 5061** per la linea ACE 8

Identificazione: Messaggi syslog elenco accessi firewall

Il messaggio syslog del firewall *106023* verrà generato per i pacchetti negati da una voce di controllo di accesso (ACE) che non dispone della parola chiave **log**. Per ulteriori informazioni sul messaggio syslog, consultare il messaggio Cisco ASA serie 5500 System Log, 8.2 - 106023.

Le informazioni sulla configurazione del syslog per Cisco ASA serie 5500 Adaptive Security Appliance sono disponibili in Monitoraggio - configurazione della registrazione. Per informazioni sulla configurazione del syslog sul modulo FWSM per gli switch Cisco Catalyst serie 6500 e i router Cisco serie 7600, consultare il documento sul monitoraggio del modulo Firewall Services.

Nell'esempio seguente, il **comando show logging | il** comando *grep regex* estrae i messaggi syslog dal buffer di registrazione sul firewall. Questi messaggi forniscono informazioni aggiuntive sui pacchetti rifiutati che potrebbero indicare potenziali tentativi di sfruttare le vulnerabilità descritte in questo documento. È possibile utilizzare diverse espressioni regolari con la parola chiave **grep** per cercare dati specifici nei messaggi registrati.

Per ulteriori informazioni sulla sintassi delle espressioni regolari, vedere Creazione di

un'espressione regolare.

```
firewall#show logging | grep 106023
        Aug 04 2010 08:45:44: %ASA-4-106023: Deny tcp src outside:192.168.60.5/22724
            dst inside:192.168.60.21/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:44: %ASA-4-106023: Deny tcp src outside:192.168.0.4/40011
            dst inside:192.168.60.15/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:44: %ASA-4-106023: Deny tcp src
outside:192.168.208.144/61650
            dst inside:192.168.60.11/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:48: %ASA-4-106023: Deny tcp src outside:192.168.0.2/59865
            dst inside:192.168.60.31/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:48: %ASA-4-106023: Deny tcp src outside:192.168.48.42/12345

            dst inside:192.168.60.3/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:48: %ASA-4-106023: Deny tcp src
outside:192.168.126.168/5053
            dst inside:192.168.60.9/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:52: %ASA-4-106023: Deny udp src
outside:192.168.60.134/22670
            dst inside:192.168.60.11/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:52: %ASA-4-106023: Deny udp src outside:192.168.44.68/18777

            dst inside:192.168.60.13/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:52: %ASA-4-106023: Deny udp src
outside:192.68.214.152/13391
            dst inside:192.168.60.41/5061 by access-group "tACL-Policy"
        Aug 04 2010 08:45:54: %ASA-4-106023: Deny udp src outside:192.168.23.3/21826
            dst inside:192.168.60.10/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:54: %ASA-4-106023: Deny udp src
outside:192.168.34.173/29006
            dst inside:192.168.60.8/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:54: %ASA-4-106023: Deny udp src
outside:192.168.28.109/16289
            dst inside:192.168.60.99/5060 by access-group "tACL-Policy"
        Aug 04 2010 08:45:54: %ASA-4-106023: Deny udp src outside:192.168.81.251/9919

            dst inside:192.168.60.1/5060 by access-group "tACL-Policy"
firewall#
```

Nell'esempio precedente, i messaggi registrati per il *tACL-Policy* tACL mostrano pacchetti **SIP** potenzialmente oggetto di spoofing per le **porte TCP 5060 e 5061** e le **porte UDP 5060 e 5061** inviate al blocco di indirizzi assegnato ai dispositivi interessati.

Per ulteriori informazioni sui messaggi syslog per le appliance di sicurezza ASA, consultare la guida Cisco ASA serie 5500 System Log Messages, versione 8.2. Per ulteriori informazioni sui messaggi syslog per il modulo FWSM, consultare i messaggi log del sistema di registrazione dello switch Catalyst serie 6500 e del router Cisco serie 7600 Firewall Services Module.

Per ulteriori informazioni sull'analisi degli incidenti tramite eventi syslog, consultare il white paper Identificazione degli incidenti tramite firewall e eventi syslog del router IOS Applicati Intelligence.

Identificazione: protezione da spoofing con inoltro percorso inverso unicast

Il messaggio syslog del firewall *106021* verrà generato per i pacchetti negati da RPF unicast. Per ulteriori informazioni sul messaggio syslog, consultare il messaggio Cisco ASA serie 5500 System Log, 8.2 - 106021.

Le informazioni sulla configurazione del syslog per Cisco ASA serie 5500 Adaptive Security Appliance sono disponibili in Monitoraggio - configurazione della registrazione. Per informazioni sulla configurazione del syslog sul modulo FWSM per gli switch Cisco Catalyst serie 6500 e i router Cisco serie 7600, consultare il documento sul monitoraggio del modulo Firewall Services.

Nell'esempio seguente, il **comando show logging | il** comando *grep regex* estrae i messaggi syslog dal buffer di registrazione sul firewall. Questi messaggi forniscono informazioni aggiuntive sui pacchetti rifiutati che potrebbero indicare potenziali tentativi di sfruttare le vulnerabilità descritte in questo documento. È possibile utilizzare diverse espressioni regolari con la parola chiave **grep** per cercare dati specifici nei messaggi registrati.

Per ulteriori informazioni sulla sintassi delle espressioni regolari, vedere Creazione di un'espressione regolare.

```
firewall#show logging | grep 106021
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.202 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.126 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.22 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.75 to 192.168.60.1 on interface outside
        Aug 04 2010 08:52:46: %ASA-1-106021: Deny UDP reverse path check from
            192.168.60.248 to 192.168.60.1 on interface outside
```

Il comando **show asp drop** può identificare anche il numero di pacchetti scartati dalla funzione RPF unicast, come mostrato nell'esempio che segue:

```
firewall#show asp drop frame rpf-violated
  Reverse-path verify failed (rpf-violated)                    10
```

Nell'esempio precedente, Unicast RPF ha scartato **10 pacchetti IP** ricevuti su interfacce con Unicast RPF configurato. La mancanza di output indica che la funzionalità RPF unicast sul firewall non ha scartato pacchetti.

Per ulteriori informazioni sul debug di pacchetti o connessioni ignorati dai percorsi di sicurezza accelerati, vedere la guida di riferimento dei comandi di Cisco Security Appliance per show asp drop.

Cisco Intrusion Prevention System

Attenuazione: azioni evento firma Cisco IPS

Gli amministratori possono utilizzare gli accessori e i moduli di servizi IPS (Cisco Intrusion Prevention System) per rilevare le minacce e contribuire a prevenire i tentativi di sfruttare le vulnerabilità descritte più avanti nel documento. Queste vulnerabilità possono essere rilevate dalle seguenti firme:

- 29219-0 CUCM Formato non valido del messaggio REGISTER DoS
- 29239-0 Vulnerabilità corruzione memoria Cisco CUP

29219-0 CUCM Formato non valido del messaggio REGISTER DoS

A partire dall'aggiornamento della firma S510 per i sensori che eseguono Cisco IPS versione 6.x e successive, questa vulnerabilità può essere rilevata dalla firma 29219/0 (Nome firma: CUCM Formato non valido REGISTER Message DoS). La firma 29219/0 è abilitata per impostazione predefinita, attiva un evento di gravità *Medio*, ha un indice di fedeltà della firma (SFR) di 90 ed è configurata con un'azione evento predefinita **produce-alert**.

Questa firma viene attivata dopo il rilevamento di un messaggio SIP REGISTER non valido che può causare un rifiuto del servizio in Cisco Unified Communications Manager. La vulnerabilità è documentata nell'ID bug Cisco CSCtf66305 ed è stata assegnata all'identificatore CVE CVE-2010-2838. L'attivazione di questa firma può indicare un potenziale utilizzo di questa vulnerabilità.

29239-0 Vulnerabilità corruzione memoria Cisco CUP

A partire dall'aggiornamento della firma S510 per i sensori con Cisco IPS versione 6.x e successive, questa vulnerabilità può essere rilevata dalla firma 29239/0 (nome firma: Cisco CUP Memory Corruption Vulnerability). La firma 29239/0 è abilitata per impostazione predefinita, attiva un evento di *alta* gravità, ha un indice di fedeltà della firma (SFR) di 90 ed è configurata con un'azione evento predefinita di **produce-alert**.

Questa firma viene attivata sui tentativi di sfruttare un bug di danneggiamento della memoria presente in Cisco CUP utilizzando la porta TCP 5070. La vulnerabilità è documentata nell'ID bug Cisco CSCtd39629 ed è stata assegnata all'identificatore CVE CVE-2010-2840. L'attivazione di questa firma può indicare un potenziale utilizzo di questa vulnerabilità.

Gli amministratori possono configurare i sensori Cisco IPS in modo da eseguire un'azione evento quando viene rilevato un attacco. L'azione evento configurata esegue controlli preventivi o deterrenti per contribuire alla protezione da un attacco che tenta di sfruttare le vulnerabilità descritte in questo documento.

I sensori Cisco IPS sono più efficaci se installati in modalità di protezione inline combinata con l'uso di un'azione evento. La funzione di prevenzione automatica delle minacce per i sensori Cisco IPS 6.x e versioni successive distribuiti in modalità di protezione inline fornisce una prevenzione delle minacce contro gli attacchi che tentano di sfruttare le vulnerabilità descritte in questo documento. La prevenzione delle minacce viene ottenuta tramite un override predefinito che esegue un'azione evento per le firme attivate con un valore *riskRatingValue* maggiore di 90.

Per ulteriori informazioni sul calcolo del rating di rischio e della minaccia, fare riferimento a Rating di rischio e Rating di minaccia: Semplificare la gestione delle policy IPS.

Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco

Identificazione: Cisco Security Monitoring, Analysis, and Response System Incident

L'appliance Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) può creare incidenti relativi a eventi correlati alle vulnerabilità descritte in questo documento utilizzando le firme IPS 29219-0 (nome firma: CUCM Malformed REGISTER Message DoS) e 29239-0 (nome firma: Cisco CUP Memory Corruption Vulnerability). Una volta scaricato l'aggiornamento della firma dinamica S510, utilizzando le parole chiave **NR-29219/0** per la firma IPS 29219/0 e **NR-29239/0** per la firma IPS 29239/0 e un tipo di query **All Matching Event Raw Messages** sull'appliance Cisco Security MARS è disponibile un report in cui sono elencati gli

incidenti creati dalla firma IPS.

A partire dalle versioni 4.3.1 e 5.3.1 degli accessori Cisco Security MARS, è stato aggiunto il supporto per la funzionalità di aggiornamento dinamico delle firme di Cisco IPS. Questa funzionalità consente di scaricare nuove firme da Cisco.com o da un server Web locale, di elaborare e classificare correttamente gli eventi ricevuti che corrispondono a tali firme e di includerli nelle regole di ispezione e nei report. Questi aggiornamenti forniscono la normalizzazione degli eventi e la mappatura dei gruppi di eventi e consentono inoltre all'accessorio MARS di analizzare le nuove firme provenienti dai dispositivi IPS.

Attenzione: se gli aggiornamenti dinamici delle firme non sono configurati, gli eventi che corrispondono a queste nuove firme vengono visualizzati come *tipi di evento sconosciuti* nelle query e nei report. Poiché MARS non include questi eventi nelle regole di ispezione, gli incidenti possono non essere creati per potenziali minacce o attacchi che si verificano all'interno della rete.

Per impostazione predefinita, questa funzionalità è abilitata ma richiede la configurazione. Se non è configurata, verrà attivata la seguente regola Cisco Security MARS:

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

Quando questa funzionalità è attivata e configurata, gli amministratori possono determinare la versione della firma corrente scaricata da MARS selezionando **? > Informazioni su** e rivedendo il valore *Versione firma IPS*.

Per le versioni Cisco Security MARS 4.3.1 e 5.3.1 sono disponibili informazioni aggiuntive sugli aggiornamenti dinamici delle firme e istruzioni per la configurazione degli aggiornamenti dinamici delle firme.

Ulteriori informazioni

Cronologia delle revisioni

Revisione 1.0	2010-agosto-25	Versione pubblica iniziale

Procedure di sicurezza di Cisco

Le informazioni complete sulla segnalazione delle vulnerabilità della sicurezza nei prodotti Cisco, su come ottenere assistenza in caso di incidenti relativi alla sicurezza e su come registrarsi per ricevere informazioni sulla sicurezza da Cisco, sono disponibili sul sito Web di Cisco all'indirizzo https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html. Ciò include istruzioni per le richieste della stampa relative agli avvisi di sicurezza Cisco. Tutti gli avvisi sulla sicurezza Cisco sono disponibili all'indirizzo http://www.cisco.com/go/psirt.

Informazioni correlate

- Bollettini sulla mitigazione applicata da Cisco
- Cisco Security
- Servizio Cisco Security IntelliShield Alert Manager
- Guida Cisco per fortificare i dispositivi Cisco IOS
- Informazioni sui vettori di minaccia XSS (Cross-Site Scripting)
- Cisco IOS NetFlow - Home Page su Cisco.com
- White paper su Cisco IOS NetFlow
- Analisi delle prestazioni di NetFlow
- White paper su Cisco Network Foundation Protection
- Presentazioni di Cisco Network Foundation Protection
- Identificazione e mitigazione degli attacchi TTL in scadenza
- Un approccio orientato alla sicurezza per l'indirizzamento IP
- Contromisure per l'utilizzo dannoso delle intestazioni di routing IPv6 di tipo 0
- Prodotti Cisco Firewall - Home Page su Cisco.com
- Miglioramenti unicast Reverse Path Forwarding per il provider di servizi Internet
- Cisco Intrusion Prevention System
- Download di firme IPS Cisco
- Pagina di ricerca delle firme IPS Cisco
- Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco
- Vulnerabilità ed esposizioni comuni (CVE)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).