Identificazione e mitigazione dello sfruttamento delle vulnerabilità di Denial of Service in Cisco Unified Communications Manager e Cisco Intercompany Media Engine

Identificazione e mitigazione dello sfruttamento delle vulnerabilità di Denial of Service in Cisco Unified Communications Manager e Cisco Intercompany Media Engine

ID advisory: cisco-amb-20110824-cucm-ime

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110824-cucm-ime

Revisione 1.1

Ultimo aggiornamento: 2 novembre 2011 23:20 UTC (GMT)

Per la Pubblica Release 2011 Agosto 24 00:00 UTC (GMT)

Sommario

Risposta di Cisco

Questo Bollettino sulla mitigazione applicata è un documento complementare ai consigli sulla sicurezza PSIRT *Vulnerabilità* e *vulnerabilità Denial of Service di Cisco Unified Communications Manager* e *Denial of Service in Cisco Intercompany Media Engine* e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

Cisco Unified Communications Manager e Intercompany Media Engine presentano diverse vulnerabilità. Le seguenti sottosezioni riepilogano queste vulnerabilità:**Vulnerabilità DoS in Cisco Unified Communications Manager con il servizio Packet Capture abilitato:** questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza interazione dell'utente finale. Se questa vulnerabilità viene sfruttata correttamente, il dispositivo interessato potrebbe bloccarsi. I ripetuti tentativi di sfruttare questa

vulnerabilità potrebbero causare una condizione di Denial of Service (DoS) prolungata, esaurendo la memoria di Unified Communications Manager. Il vettore di attacco per l'utilizzo è tramite pacchetti TCP che completano un handshake TCP a 3 vie per Unified Communications Manager e lasciano le connessioni aperte.A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-2560.**Vulnerabilità DoS in Cisco Unified Communications Manager con determinate configurazioni di MTP:** questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. Se questa vulnerabilità viene sfruttata correttamente, il dispositivo interessato potrebbe bloccarsi. Ripetuti tentativi di sfruttare questa vulnerabilità potrebbero causare una condizione DoS prolungata.I vettori di attacco per l'utilizzo sono attraverso pacchetti che utilizzano i seguenti protocolli e porte:

- Session Initiation Protocol (SIP) con porta TCP 5060
- SIP over Transport Layer Security (TLS) 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 questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-2561.**Vulnerabilità DoS in Cisco Unified Communications Manager durante l'elaborazione di alcuni messaggi SIP INVITE:** questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. Se questa vulnerabilità viene sfruttata correttamente, il dispositivo interessato potrebbe bloccarsi. Ripetuti tentativi di sfruttare questa vulnerabilità potrebbero causare una condizione DoS prolungata.I vettori di attacco per l'utilizzo sono attraverso pacchetti che utilizzano i seguenti protocolli e porte:

- SIP con porta TCP 5060
- SIP-TLS over Transport Layer Security (TLS) con porta TCP 5061
- SIP con porta UDP 5060
- SIP-TLS con porta UDP 5061

Un utente non autorizzato potrebbe sfruttare queste vulnerabilità utilizzando pacchetti di spoofing.A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-2562.**Due vulnerabilità DoS in Cisco Unified Communications Manager e Cisco Intercompany Media Engine (IME) con Service Advertisement Framework (SAF):** questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza interazione dell'utente finale. Se questa vulnerabilità viene sfruttata correttamente, il dispositivo interessato potrebbe bloccarsi. Ripetuti tentativi di sfruttare questa vulnerabilità potrebbero causare una condizione DoS prolungata.I vettori di attacco per lo sfruttamento sono attraverso i mezzi artigianali:

- Pacchetti SAF con porte TCP 5050 (per Cisco Unified Communications Manager)
- Pacchetti SAF che utilizzano la porta TCP 5620 (per IME)

A queste vulnerabilità sono stati assegnati gli identificatori CVE CVE-2011-2563 e CVE-2011-2564.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-20110824-cucm e https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110824-ime.

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 può fornire mezzi efficaci di prevenzione degli attacchi utilizzando 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.Poiché esiste la possibilità che un client di rete attendibile venga influenzato da un worm che non utilizza pacchetti con indirizzi di origine oggetto di spoofing, RPF e IPSG unicast non forniscono una protezione completa da queste vulnerabilità.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.

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

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'appliance e il modulo Cisco ACE Application Control Engine possono fornire un'efficace prevenzione degli attacchi tramite la normalizzazione TCP.Questo meccanismo di protezione filtra e scarta i 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.Il software Cisco IOS, Cisco ASA, i firewall FWSM, l'appliance e il modulo Cisco ACE Application Control Engine 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

Si consiglia alle organizzazioni di seguire i processi standard di valutazione e mitigazione dei rischi per determinare l'impatto potenziale di [questa vulnerabilità|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 ACE
- 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 i pacchetti SIP, SAF e SIP-TLS non autorizzati sulle porte TCP e UDP 5060 e 5061 inviati ai dispositivi interessati. Nell'esempio seguente, 192.168.60.0/24 e 2001:DB8:1:60::/64 sono rispettivamente lo spazio di indirizzi IPv4 e IPv6 utilizzato dai dispositivi interessati e l'host in 192.168.100.1 (2001:DB8:1:100::1 per IPv6) 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 protocols and 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 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5050 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5620 ! !-- The following vulnerability-specific access control entries !-- (ACEs) can aid in identification of attacks ! access-list 150 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5061 access-list 150 deny deny udp any 192.168.60.0 0.0.0.255 eq 5060 access-list 150 deny deny udp any 192.168.60.0 0.0.0.255 eq 5061 access-list 150 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5050 access-list 150 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5620 ! !-- 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 ! !-- Create the corresponding IPv6 tACL ! ipv6 access-list
IPv6-Infrastructure-ACL-Policy ! !-- Include explicit permit statements for
trusted sources !-- that require access on the vulnerable protocols and ports
! permit tcp host 2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5060 permit tcp
host 2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5061 permit udp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5060 permit udp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5061 permit tcp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5050 permit tcp host
2001:DB8:1:100::1 2001:DB8:1:60::/64 eq 5620 ! !-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in
identification of attacks to global and !-- link local addresses ! deny tcp
any 2001:DB8:1:60::/64 eq 5060 deny tcp any 2001:DB8:1:60::/64 eq 5061 deny
udp any 2001:DB8:1:60::/64 eq 5060 deny udp any 2001:DB8:1:60::/64 eq 5061
deny tcp any 2001:DB8:1:60::/64 eq 5050 deny tcp any 2001:DB8:1:60::/64 eq
5620 ! !-- Permit other required traffic to the infrastructure address !--
range and allow IPv6 Neighbor Discovery packets, which !-- include Neighbor
Solicitation packets and Neighbor !-- Advertisement packets ! permit icmp any
any nd-ns permit icmp any any nd-na ! !-- Explicit deny for all other IP
traffic to the global !-- infrastructure address range ! deny ipv6 any
2001:DB8:1:60::/64 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic
!-- in accordance with existing security policies and configurations ! ! !--
Apply tACLs to interfaces in the ingress direction ! interface
GigabitEthernet0/0 ip access-group 150 in ipv6 traffic-filter IPv6-
Infrastructure-ACL-Policy 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 rispetto all'impostazione predefinita utilizzando il comando di configurazione globale **ip icmp rate-limit** *unreachableinterval-in-ms*.**Attenuazione: protezione da spoofingInoltro 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 e SIP-TLS sulle porte TCP e 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
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
    30 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
```

```
    40 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
    50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5050
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5620
    70 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (5 matches)
    80 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (2 matches)
    90 deny deny udp any 192.168.60.0 0.0.0.255 eq 5060 (7 matches)
    100 deny deny udp any 192.168.60.0 0.0.0.255 eq 5061 (4 matches)
    110 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5050 (6 matches)
    120 deny deny tcp any 192.168.60.0 0.0.0.255 eq 5620 (1 matches)
    130 permit icmp any any nd-ns
    140 permit icmp any any nd-ns
    150 deny ip any any
router#
```

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

- **5** pacchetti **SIP** sulla **porta TCP 5060** per la linea ACE 70
- **2** pacchetti **SIP-TLS** sulla **porta TCP 5061** per la linea ACE 80
- **7** pacchetti **SIP** sulla **porta UDP 5060** per la linea ACE 90
- **4** pacchetti **SIP** sulla **porta UDP 5061** per la linea ACE 100
- **6** pacchetti **SAF** sulla **porta TCP 5050** per la linea ACE 110
- **1** pacchetto **SAF** sulla **porta TCP 5620** per la linea ACE 120

L'output corrispondente per gli ACL IPv6 è molto simile e verrà omesso per brevità. 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 dell'elenco di controllo di accesso 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/portinternal,* **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 command | begin** *regex* **e show command | include i modificatori del comando regex** sono 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 Forwarding Information Base di Cisco Express Forwarding.**Cisco IOS NetFlowIdentificazione: 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 (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 ager 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         192.168.10.201  Gi0/1         192.168.60.102  06 0984 13C4     3
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 13C5     2
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3A 13BA     6
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 13C4     2
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B31 15F4     1
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   11 0B89 13C5     7
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 13C4     4
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
router#
```

Nell'esempio precedente, sono presenti più flussi per i pacchetti SIP, SAF e SIP-TLS sulle porte TCP 5060 (valore esadecimale 13C4), 5061 (valore esadecimale 13C5), 5050 (valore esadecimale 13BA) e 5620 (valore esadecimale 15F4) e le porte UDP 5060 (valore esadecimale 13C4) e **5** .Il 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 e SIP-TLS inviato sulle porte UDP 5060 e 5061 e di analizzare i flussi per determinare se provengono da host o reti non attendibili.Per visualizzare solo i flussi di traffico per i pacchetti SIP, SAF e SIP-TLS sulle porte TCP 5060 (valore esadecimale 13C4), 5061 (valore esadecimale 13C5), 5050 (valore esadecimale 13BA) e 5620 (valore esadecimale 15F4), eseguire il comando **show ip cache flow | include SrcIf|_06_.*(13C4|13C5|13BA|15F4)_** visualizzerà i record NetFlow UDP correlati, come mostrato di seguito:**Flussi TCP**

```
router#show ip cache flow | include SrcIf|_06_.*(13C4|13C5|13BA|15F4)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  06 0984 13C4     3
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3E 13C5     2
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B3A 13BA     6
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 13C4     2
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   06 0B31 15F4     1
router#
```

Per visualizzare solo i flussi di traffico per i pacchetti SIP e SIP-TLS sulle porte UDP 5060 (valore esadecimale 13C4) e 5061 (valore esadecimale 13C5), usare il comando **show ip cache flow | include SrcIf|_11_.*(13C4|13C5)_** visualizzerà i record NetFlow UDP correlati, come mostrato di seguito:**Flussi UDP**

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   11 0B89 13C5     7
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 13C4     4
router#
```

Identificazione: identificazione del flusso di traffico mediante i record NetFlow IPv6 Gli amministratori possono configurare Cisco IOS IPv6 NetFlow sui router e gli switch Cisco IOS per aiutare a identificare i flussi di traffico che potrebbero essere tentativi di sfruttare le vulnerabilità descritte in questo documento. 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.Questo output viene generato da un dispositivo Cisco IOS con software Cisco IOS versione 12.4 e treno principale. La sintassi del comando può variare a seconda della famiglia di prodotti software Cisco IOS.

```
router#show ipv6 flow cache
IP packet size distribution (50078919 total packets):
   1-32  64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .990 .001 .008 .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, 475168 bytes
  8 active, 4088 inactive, 6160 added
  1092984 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  IP Sub Flow Cache, 33928 bytes
  16 active, 1008 inactive, 12320 added, 6160 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added

SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x06 0x2001 0x13C4 1464K
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x180A 0x13C5 3456
2001:DB...6A:5BA6 Gi0/0    2001:DB...28::21 Gi0/1    0x3A 0x0000 0x8000 2191
2001:DB...6A:5BA6 Gi0/0    2001:DB...134::3 Gi0/1    0x3A 0x0000 0x8000 1909
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x18C4 0x13C4 4567K
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::4 Gi0/1    0x3A 0x0000 0x8000 1192
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::2 Gi0/1    0x06 0x160A 0x13C5 1597
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::3 Gi0/1    0x06 0x1610 0x13BA 1001
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::4 Gi0/1    0x06 0x1634 0x15F4 1292
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::3 Gi0/1    0x3A 0x0000 0x8000 1292
2001:DB...6A:5BA6 Gi0/0    2001:DB...146::3 Gi0/1    0x3A 0x0000 0x8000 1392
2001:DB...6A:5BA6 Gi0/0    2001:DB...144::4 Gi0/1    0x3A 0x0000 0x8000 1493
```

Per consentire la visualizzazione dell'indirizzo IPv6 completo a 128 bit, utilizzare il comando **terminal width 132** in modalità di esecuzione.Nell'esempio precedente, sono presenti più flussi per i pacchetti SIP, SAF e SIP-TLS sulle porte TCP 5060 (valore esadecimale 13C4), 5061 (valore esadecimale 13C5), 5050 (valore esadecimale 13BA) e 5620 (valore esadecimale 15F4) e le porte UDP 5060 (valore esadecimale 13C4) e **5** .Il traffico ha origine e viene inviato agli indirizzi del blocco di indirizzi 2001:DB8:1:60::/64, 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 e SIP-TLS inviato sulle porte UDP 5060 e 5061 e di analizzare i flussi per determinare se provengono da host o reti non attendibili.Come mostrato nell'esempio che segue, per visualizzare solo i pacchetti SIP, SAF e SIP-TLS sulle porte TCP 5060 (valore esadecimale 13C4), 5061 (valore esadecimale 13C5), 5050 (valore esadecimale 13BA) e 5620 (valore esadecimale 15F4), utilizzare il comando **show ipv6 flow cache | include il** comando **SrcAddress|_06_.*(13C4|13C5|13BA|15F4)_** per visualizzare i record NetFlow correlati:**Flussi TCP**

```
router#show ipv6 flow cache | include SrcIf|_06_.*(13C4|13C5|13BA|15F4)_
SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x06 0x2001 0x13C4 1464K
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::2 Gi0/1    0x06 0x160A 0x13C5 1597
2001:DB...6A:5BA6 Gi0/0 2001:DB...128::3 Gi0/1 0x06 0x1610 0x13BA 1001
2001:DB...6A:5BA6 Gi0/0    2001:DB...128::4 Gi0/1    0x06 0x1634 0x15F4 1292
router#
```

Come mostrato nell'esempio seguente, per visualizzare solo i flussi di traffico SIP e SIP-TLS per la porta UDP IPv6 5060 **(valore esadecimale 0x13C4)** e 5061 **(valore esadecimale 0x13C5)**utilizzare la **show ipv6 flow cache | include il** comando **SrcAddress|_11_.*(13C4|13C5)_** per visualizzare i record NetFlow correlati:**Flussi UDP**

```
router#show ip cache flow | include SrcIf|_11_.*(13C4|13C5)_
SrcAddress        InpIf    DstAddress       OutIf    Prot SrcPrt DstPrt Packets
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x180A 0x13C5 3456
2001:DB...06::201 Gi0/0    2001:DB...28::20 Local    0x11 0x18C4 0x13C4 4567K
routter#
```

Cisco ASA e firewall FWSMAttenuazione: 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 i pacchetti SIP, SAF e SIP-TLS non autorizzati sulle porte TCP e UDP 5060 e 5061 inviati ai dispositivi interessati. Nell'esempio seguente, 192.168.60.0/24 e 2001:DB8:1:60:/64 è lo spazio di indirizzi IPv4 e IPv6, rispettivamente, utilizzato dai dispositivi interessati e l'host in 192.168.100.1 (2001:DB8:1:100::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 protocols and 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 access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5050 access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 5620 ! !-- 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 access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 5050 access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 5620 ! !-- 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 ! !-- Include explicit permit statements for trusted sources !-- that require access on the vulnerable protocols and ports ! ipv6 access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-Policy permit udp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy permit udp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5050 ipv6 access-list IPv6-tACL-Policy permit tcp host 2001:DB8:1:100::1 2001:db8:1:60::/64 eq 5620 ! !-- The following vulnerability-specific access control entries !-- (ACEs) can aid in identification of attacks ! ipv6 access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-Policy deny udp any 2001:db8:1:60::/64 eq 5060 ipv6 access-list IPv6-tACL-Policy deny udp any 2001:db8:1:60::/64 eq 5061 ipv6 access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5050 ipv6 access-list IPv6-tACL-Policy deny tcp any 2001:db8:1:60::/64 eq 5620 ! !-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing security policies and configurations ! !-- Explicit deny for all other IP traffic ! ipv6 access-list IPv6-Transit-ACL-Policy deny ip any any ! !-- Apply tACLs to interfaces in the ingress direction ! access-group tACL-Policy in interface outside access-group IPv6-Transit-ACL-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.
Attenuazione: normalizzazione TCP La funzione di normalizzazione TCP identifica i pacchetti anomali sui quali l'appliance di sicurezza può intervenire quando vengono rilevati; ad esempio, l'appliance di sicurezza può consentire, eliminare o cancellare i pacchetti. Il normalizzatore TCP include azioni non configurabili e azioni configurabili. In genere, le azioni non configurabili che interrompono o cancellano le connessioni si applicano ai pacchetti considerati dannosi. La normalizzazione TCP è disponibile a partire dal software versione 7.0(1) per Cisco ASA serie 5500 Adaptive Security Appliance e nella versione 3.1(1) per il modulo Firewall Services.La normalizzazione TCP è abilitata per impostazione predefinita e scarta i pacchetti che possono sfruttare queste vulnerabilità. La protezione dai pacchetti che potrebbero sfruttare queste vulnerabilità è un'azione di normalizzazione TCP non configurabile. Per abilitare questa funzionalità non sono necessarie modifiche alla configurazione.La funzione di normalizzazione TCP può essere utilizzata per limitare il limite delle connessioni simultanee e il timeout di inattività per le connessioni TCP a Cisco Unified Communications Manager, impedendo in tal modo la condizione DoS. I limiti devono essere configurati in base al numero massimo normale di connessioni osservate verso Cisco Unified Communications Manager. Si noti che la configurazione del normalizzatore TCP per impedire un numero anormale di connessioni a Cisco Unified Communications Manager non impedirà a un utente malintenzionato di esaurire il numero consentito di connessioni, ma impedirà a Cisco Unified Communications Manager di esaurire la memoria a causa di molte connessioni inattive.**Nota:** prestare attenzione ai limiti impostati in ogni ambiente, in quanto potrebbero negare le connessioni legittime se non sono impostate per aderire ai limiti massimi legittimi per l'ambiente specifico.Nell'esempio seguente, 192.168.60.200/24 è l'indirizzo IP del dispositivo interessato. La configurazione limita a 1000 le connessioni simultanee TCP al dispositivo e imposta il timeout di inattività della connessione a 30 minuti. È necessario prestare attenzione ai limiti impostati in ogni ambiente, in quanto potrebbero negare connessioni legittime se non sono impostati per aderire ai normali limiti massimi per l'ambiente specifico.

```
! !-- Match TCP traffic to the Cisco Unified Communications Manager ! access-list CVE-2011-2560-acl extended permit tcp any host 192.168.60.200 class-map CVE-2011-2560-cm match access-list CVE-2011-2560-acl ! !-- Configure the connection limits for TCP !-- traffic to the Cisco Unified Communications Manager ! policy-map global_policy class CVE-2011-2560-cm set connection conn-max 1000 set connection timeout idle 0:30:00 service-policy global_policy global
```

Per ulteriori informazioni sulla normalizzazione TCP, consultare la sezione Configurazione della normalizzazione TCP in Cisco ASA serie 5500 Configuration Guide using the CLI, 8.2.**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 e SIP-TLS sulle porte TCP e UDP 5060 e 5061 che sono stati 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=34)
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=24)
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=4)
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=2)
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq sip (hitcnt=44)
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=61)
access-list tACL-Policy line 7 extended deny tcp any
     192.168.60.0 255.255.255.0 eq sip (hitcnt=5)
access-list tACL-Policy line 8 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=2)
access-list tACL-Policy line 9 extended deny udp any
     192.168.60.0 255.255.255.0 eq sip (hitcnt=7)
access-list tACL-Policy line 10 extended deny udp any
     192.168.60.0 255.255.255.0 eq 5061 (hitcnt=4)
```

```
access-list tACL-Policy line 11 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5050 (hitcnt=6)
access-list tACL-Policy line 12 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 5620 (hitcnt=1)
access-list tACL-Policy line 13 extended deny ip any any (hitcnt=8)
firewall#
```

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

- **5** pacchetti **SIP** sulla **porta TCP 5060** per la linea ACE 7
- **2** pacchetti **SIP-TLS** sulla **porta TCP 5061** per la linea ACE 8
- **7** pacchetti **SIP** sulla **porta UDP 5060** per la linea ACE 9
- **4** pacchetti **SIP** sulla **porta UDP 5061** per la linea ACE 10
- **6** pacchetti **SAF** sulla **porta TCP 5050** per la linea ACE 11
- **1** pacchetto **SAF** sulla **porta TCP 5620** per la linea ACE 12

L'output corrispondente per gli ACL IPv6 è molto simile e verrà omesso per brevità.**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 28 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2924
         dst inside:192.168.60.191/sip by access-group "tACL-Policy"
  Aug 28 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/5061 by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.19/2934
         dst inside:192.168.60.191/sip by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny udp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/5061 by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/3961
         dst inside:192.168.60.197/5050 by access-group "tACL-Policy"
  Aug 24 2011 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.201/2939
         dst inside:192.168.60.185/5620 by access-group "tACL-Policy"
firewall#
```

Nell'esempio precedente, i messaggi registrati per il *tACL-Policy* tACL mostrano pacchetti **SIP e SIP-TLS** potenzialmente oggetto di spoofing per le **porte TCP e 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 24 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Aug 24 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Aug 24 2010 00:15:13: %ASA-1-106021: Deny TCP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
```

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                      11
firewall#
```

Nell'esempio precedente, Unicast RPF ha scartato **11 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.**Identificazione: Normalizzazione TCP**Per le appliance Cisco ASA serie 5500 Adaptive Security, il comando **show service-policy** può identificare il numero di pacchetti ignorati dalla funzione di normalizzazione TCP, come mostrato nell'esempio che segue:

```
firewall#  show service-policy set connection detail

Global policy:
  Service-policy: global_policy
    Class-map: CVE-2011-2560-cm
      Set connection policy: conn-max 1000
        current conns 15, drop 5
      Set connection timeout policy:
        idle 0:30:00
        DCD: disabled, retry-interval 0:00:15, max-retries 5
        DCD: client-probe 0, server-probe 0, conn-expiration 0            11
firewall#
```

Nell'esempio precedente, la normalizzazione TCP ha interrotto **5 nuove connessioni** che superavano il limite di connessione.**Cisco ACE****Attenuazione: normalizzazione TCP**La normalizzazione TCP è una funzionalità di layer 4 costituita da una serie di controlli che Cisco ACE esegue nelle varie fasi di un flusso, a partire dall'impostazione iniziale della connessione fino alla chiusura di una connessione. Molti controlli dei segmenti possono essere controllati o modificati configurando una o più impostazioni di connessione TCP avanzate. La voce ACE utilizza queste impostazioni di connessione TCP per decidere quali controlli eseguire e se eliminare un segmento TCP in base ai risultati dei controlli. La voce ACE elimina i segmenti che appaiono anormali o in formato non corretto.La normalizzazione TCP è abilitata per impostazione predefinita e scarta i pacchetti che possono sfruttare queste vulnerabilità. La protezione dai pacchetti che potrebbero sfruttare queste vulnerabilità è un'azione di normalizzazione TCP non configurabile; per abilitare questa funzionalità non sono necessarie modifiche alla configurazione.La funzione di normalizzazione TCP può essere utilizzata per limitare il limite di connessioni simultanee, la velocità di connessione e il timeout di inattività per le connessioni TCP a Cisco Unified Communications Manager, impedendo in tal modo la condizione DoS. I limiti devono essere configurati in base al numero massimo normale e alla velocità di connessioni osservate verso Cisco Unified Communications Manager. Si noti che la configurazione del normalizzatore TCP per impedire un numero anormale di connessioni a Cisco Unified Communications Manager non impedirà a un utente malintenzionato di esaurire il numero consentito di connessioni, ma impedirà a Cisco Unified Communications Manager di esaurire la memoria a causa di molte connessioni inattive.**Nota:** prestare attenzione ai limiti impostati in ogni ambiente, in quanto potrebbero negare le connessioni legittime se non sono impostate per aderire ai limiti massimi legittimi per l'ambiente specifico.Nell'esempio seguente, 192.168.60.200/24 è l'indirizzo IP del dispositivo interessato. La configurazione limita le connessioni simultanee TCP al dispositivo a 1000, la velocità di connessione a 100000 connessioni al secondo e imposta il timeout di inattività della connessione a 30 minuti.

```
! !-- Create a connection parameter map to group together TCP/IP !--
normalization and termination parameters ! parameter-map type connection CVE-
2011-2560-parameter-map limit-resource conc-connections 1000 set timeout
inactivity 1800 rate-limit connection 100000 ! !-- Match TCP traffic to the
Cisco Unified Communications Manager ! class-map match-any CVE-2011-2560-cm
match destination-address 192.168.60.200 ! !-- Configure the connection
limits for TCP !-- traffic to the Cisco Unified Communications Manager !
policy-map multi-match CVE-2011-2560_policy class CVE-2011-2560-cm connection
```

```
advanced-options CVE-2011-2560-parameter-map ! !-- Apply the policy to the interface ! interface vlan 50 service-policy input CVE-2011-2560_policy
```

Per ulteriori informazioni sulla normalizzazione TCP, consultare la sezione Configurazione della normalizzazione TCP/IP e dei parametri di riassemblaggio IP in Cisco ACE 4700 Series Appliance Security Configuration Guide.**Identificazione: Normalizzazione TCP**L'appliance e il modulo Cisco ACE Application Control Engine non forniscono l'output del comando show per i pacchetti scartati durante il tentativo di sfruttare queste vulnerabilità.**Cisco Intrusion Prevention System****Attenuazione: azioni evento firma Cisco IPS**Gli amministratori possono utilizzare gli accessori e i moduli servizi di Cisco Intrusion Prevention System (IPS) per rilevare le minacce e contribuire a prevenire i tentativi di sfruttare una delle vulnerabilità descritte in questo documento. A partire dall'aggiornamento della firma S590 per i sensori con Cisco IPS versione 6.x e successive, la vulnerabilità può essere rilevata dalla firma 38386/0(Nome firma: Cisco Intercompany Media Engine Denial Of Service). La firma 38386/0 è abilitata per impostazione predefinita, attiva un evento di gravità *Medio*, ha un indice di fedeltà della firma (SFR) di 15 ed è configurata con un'azione evento predefinita **di Genera avviso**.La firma 38386/0 viene attivata quando vengono rilevati pacchetti dannosi specifici inviati tramite la porta TCP 5620. L'attivazione di questa firma può indicare un potenziale sfruttamento di queste 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.Gli attacchi che utilizzano indirizzi IP oggetto di spoofing possono causare un'azione evento configurata per negare inavvertitamente il traffico proveniente da fonti attendibili.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 la firma IPS 38386/0 (nome della firma: Cisco Intercompany Media Engine Denial Of Service). Dopo il download dell'aggiornamento della firma dinamica S590, utilizzando la parola chiave **NR-38386/0** per la firma IPS 38386/0 e il tipo di query < **All Matching Events | All Matching Event Raw Messages>** sull'appliance Cisco Security MARS fornirà 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 funzione è abilitata 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 1.1	2011-2 novembre	URL documento corretto
Revisione 1.0	2011-agosto-24	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
- 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
- Prodotti Cisco Firewall - Home Page su Cisco.com
- Documentazione del modulo Cisco ACE Application Control Engine
- 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).