Identificazione e mitigazione dello sfruttamento delle molteplici vulnerabilità in Cisco Unified Communications Manager

Identificazione e mitigazione dello sfruttamento delle molteplici vulnerabilità in Cisco Unified Communications Manager

ID advisory: cisco-amb-20110427-cucm

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110427-cucm

Revisione 1.1

Per la Pubblica Release 2011 Aprile 27 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Questo bollettino sulla mitigazione applicata è un documento complementare al PSIRT Security Advisory *Multiple Vulnerabilities in Cisco Unified Communications Manager* e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

Cisco Unified Communications Manager presenta diverse vulnerabilità. Le seguenti sottosezioni riepilogano queste vulnerabilità:

Vulnerabilità Denial of Service (SIP) del Session Initiation Protocol: 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 vettori di attacco per l'utilizzo sono attraverso pacchetti 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-2011-1604, CVE-2011-1605 e CVE-2011-1606.

Vulnerabilità del caricamento file non autorizzato di Cisco Unified Reporting: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo riuscito di questa vulnerabilità può consentire a un utente non autorizzato remoto di caricare un file dannoso. Il vettore di attacco per lo sfruttamento è attraverso i pacchetti HTTPS che usano la porta TCP 8443.

A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-1607.

Vulnerabilità di SQL Injection multiple: queste vulnerabilità possono essere sfruttate in remoto con e senza autenticazione e senza interazione con l'utente finale. L'utilizzo efficace di queste vulnerabilità può consentire la divulgazione delle informazioni, che consente all'autore di un attacco di ottenere informazioni sul dispositivo interessato.

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

- HTTP con porta TCP 80
- HTTPS che utilizza la porta TCP 443
- HTTP con porta TCP 8080
- HTTPS che utilizza la porta TCP 8443

A queste vulnerabilità sono stati assegnati gli identificatori CVE CVE-2011-1609 e CVE-2011-1610.

Le informazioni sul software vulnerabile, non interessato e fisso sono disponibili in PSIRT Security Advisory, disponibile al seguente collegamento: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110427-cucm.

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.

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 i pacchetti SIP non autorizzati sulle porte TCP e UDP 5060 e 5061, i pacchetti HTTP sulle porte TCP 80 e 8080 e i pacchetti HTTPS sulle porte TCP 443 e 8443 che vengono inviati ai dispositivi interessati. 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 access-list 150 permit tcp host 192.168.100.1 192.168.60.0
0.0.0.255 eq 80 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 443 access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 ! !--
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 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 80 access-
list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 443 access-list 150 deny tcp any
192.168.60.0 0.0.0.255 eq 8080 access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq
8443 ! !-- 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 e UDP 5060 e 5061, di pacchetti HTTP sulle porte TCP 80 e 8080 e di pacchetti HTTPS sulle porte TCP 443 e 8443 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 80
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    70 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
    80 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443
    90 deny tcp any 192.168.60.0 0.0.0.255 eq 5060 (17 matches)
    100 deny tcp any 192.168.60.0 0.0.0.255 eq 5061 (19 matches)
    110 deny udp any 192.168.60.0 0.0.0.255 eq 5060 (3 matches)
    120 deny udp any 192.168.60.0 0.0.0.255 eq 5061 (49 matches)
    130 deny tcp any 192.168.60.0 0.0.0.255 eq 80 (32 matches)
    140 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (20 matches)
    150 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 (35 matches)
    160 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (10 matches)
    170 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:

- **17** pacchetti **SIP** sulla **porta TCP 5060** per la linea ACE 90
- **19** pacchetti **SIP** sulla **porta TCP 5061** per la linea ACE 100
- **3** pacchetti **SIP** sulla **porta UDP 5060** per la linea ACE 110
- **49** pacchetti **SIP** sulla **porta UDP 5061** per la linea ACE 120
- **32** pacchetti **HTTP** sulla **porta TCP 80** per la linea ACE 130
- **20** pacchetti **HTTPS** sulla **porta TCP 443** per la linea ACE 140
- **35** pacchetti **HTTP** sulla **porta TCP 8080** per la linea ACE 150
- **10** pacchetti **HTTPS** sulla **porta TCP 8443** per la linea ACE 160

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/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 | inizio comando** *regex* e **show** | include i modificatori del comando *regex* **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 (31715553 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .005 .175 .632 .032 .095 .003 .003 .003 .002 .000 .005 .002 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .020 .007 .008 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  24 active, 65512 inactive, 5451612 added
  557541771 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 533256 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet         811      0.0       137    41      0.0      32.3      16.4
TCP-FTP           2108      0.0         6    44      0.0       0.5      22.1
TCP-FTPD             5      0.0        13    52      0.0       0.7       1.5
TCP-WWW         133468      0.0         4   223      0.1       5.5      50.9
TCP-SMTP         32583      0.0         5    60      0.0      28.3      60.0
TCP-other       627608      0.1        12   175      1.8      57.8      24.1
UDP-DNS         284078      0.0         3    63      0.2      15.1      53.5
UDP-NTP          94456      0.0         1    76      0.0       0.3      60.5
UDP-Frag             1      0.0         9  1260      0.0       0.4      60.2
UDP-other      1102669      0.2         8   102      2.1      34.3      47.5
ICMP           1980458      0.4         2    89      1.1      14.3      58.5
IGMP            469264      0.1         2    37      0.2      58.2      41.0
IPINIP               2      0.0         1    76      0.0       0.0      60.4
IPv6INIP             3      0.0         1   863      0.0       0.0      60.4
GRE                  2      0.0         1   697      0.0       0.0      60.4
IP-other        724037      0.1         9    89      1.5      95.0      15.6
Total:         5451553      1.2         5   113      7.3      37.5      44.7

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  11 0984 00A1     1
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  11 0911 13C5     3
```

```
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   11 0B3E 13C4     5
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   06 0B89 13C4     1
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 13C4     1
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
Gi0/0         192.168.120.20  Gi0/1         192.168.60.102  06 0984 1F90     1
Gi0/0         192.168.12.45   Gi0/1         192.168.60.138  06 0911 13C5     3
Gi0/1         192.168.150.41  Gi0/0         192.168.60.24   06 0016 12CA     1
Gi0/0         192.168.12.87   Gi0/1         192.168.60.28   06 0B3E 0050     5
Gi0/0         192.168.10.12   Gi0/1         192.168.60.97   06 0B89 01BB     1
Gi0/0         10.88.226.8     Gi0/1         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.15   Gi0/1         192.168.60.209  06 0BD7 20FB     1
Gi0/0         10.89.16.216    Gi0/1         192.168.150.8   06 12CA 0016     1
router#
```

Nell'esempio precedente, sono presenti più flussi per il SIP sulle porte TCP 5060 (valore esadecimale 13C4) e 5061 (valore esadecimale 13C5) e le porte UDP 5060 (valore esadecimale 13C4) e 5061 (valore esadecimale 13C5) e HTTP sulle porte TCP 80 (valore esadecimale 050) e 8080 (valore esadecimale 1F90) sulle porte TCP 443 (valore esadecimale 01BB) e 8443 (valore esadecimale 20FB).

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 inviato sulla porta UDP 5060 e sulla porta 5061 e 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 UDP 5060 (valore esadecimale 13C4) e 5061 (valore esadecimale 13C5), usare il comando **show ip cache flow | include SrcIf|**_11.*(13C4|13C5) visualizza 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         192.168.12.110   Gi0/1         192.168.60.163  11 092A 13C4     6
Gi0/0         192.168.11.230   Gi0/1         192.168.60.20   11 0C09 13C4     1
Gi0/0         192.168.11.131   Gi0/1         192.168.60.245  11 0B66 13C5    18
Gi0/0         192.168.13.7     Gi0/1         192.168.60.162  11 0914 13C4     1
router#
```

Per visualizzare solo i flussi di traffico per i pacchetti SIP sulle porte TCP 5060 (valore esadecimale 13C4) e 5061 (valore esadecimale 13C5) e i pacchetti HTTP sulle porte TCP 80 (valore esadecimale 0050) e 8080 (valore esadecimale 1F90) e HTTPS sulle porte TCP 443 (valore esadecimale 01BB) e 8443 (valore esadecimale 20FB), il comando **show ip cache flow | include SrcIf|**_06_.*(13C4|13C5|0050|01BB|1F90|20FB) visualizza i record TCP NetFlow correlati, come mostrato di seguito:

Flussi TCP

```
router#show ip cache flow | include SrcIf|_06_.*(13C4|13C5|0050|01BB|1F90|20FB)
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.12.110   Gi0/1         192.168.60.163  06 092A 13C5     6
Gi0/0         192.168.11.230   Gi0/1         192.168.60.20   06 0C09 0050     1
```

```
Gi0/0          192.168.11.131   Gi0/1          192.168.60.245   06 0B66 01BB    18
Gi0/0          192.168.13.7     Gi0/1          192.168.60.162   06 0914 0050     7
Gi0/0          192.168.241.106  Gi0/1          192.168.60.27    06 0B7B 13C4    12
Gi0/0          192.168.19.222   Gi0/1          192.168.60.120   06 0C09 20FB    16
Gi0/0          192.168.12.121   Gi0/1          192.168.60.245   06 0B66 01BB    19
Gi0/0          192.168.14.17    Gi0/1          192.168.60.183   06 0914 1F90     9
Gi0/0          192.168.41.86    Gi0/1          192.168.60.217   06 0B7B 20FB     2
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 i pacchetti SIP non autorizzati sulle porte TCP e UDP 5060 e 5061, i pacchetti HTTP sulle porte TCP 80 e 8080 e i pacchetti HTTPS sulle porte TCP 443 e 8443 che vengono inviati ai dispositivi interessati. 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 sip 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 sip
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 www access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq https access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8080 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8443 ! !-
- 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 sip 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 sip 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 www access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq https access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 8080 access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 8443 ! !-- 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 e UDP 5060 e 5061, di pacchetti HTTP sulle porte TCP 80 e 8080 e di pacchetti HTTPS sulle porte TCP 443 e 8443 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; 17 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
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061
access-list tACL-Policy line 3 extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq sip
access-list tACL-Policy line 4 extended permit udp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 5061
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq www
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq https
access-list tACL-Policy line 7 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8080
access-list tACL-Policy line 8 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8443
access-list tACL-Policy line 9 extended deny tcp any 192.168.60.0 255.255.255.0 eq
sip (hitcnt=30)
access-list tACL-Policy line 10 extended deny tcp any 192.168.60.0 255.255.255.0 eq
5061 (hitcnt=43)
access-list tACL-Policy line 11 extended deny udp any 192.168.60.0 255.255.255.0 eq
sip (hitcnt=70)
access-list tACL-Policy line 12 extended deny udp any 192.168.60.0 255.255.255.0 eq
```

```
5061 (hitcnt=14)
access-list tACL-Policy line 13 extended deny tcp any 192.168.60.0 255.255.255.0 eq
www (hitcnt=45)
access-list tACL-Policy line 14 extended deny tcp any 192.168.60.0 255.255.255.0 eq
https (hitcnt=53)
access-list tACL-Policy line 15 extended deny tcp any 192.168.60.0 255.255.255.0 eq
8080 (hitcnt=70)
access-list tACL-Policy line 16 extended deny tcp any 192.168.60.0 255.255.255.0 eq
8443 (hitcnt=61)
access-list tACL-Policy line 17 extended deny tcp any any
```

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

- **30** pacchetti **SIP** sulla **porta TCP 5060** per la linea ACE 9
- **43** pacchetti **SIP** sulla **porta TCP 5061** per la linea ACE 10
- **70** pacchetti **SIP** sulla **porta UDP 5060** per la linea ACE 11
- **14** pacchetti **SIP** sulla **porta UDP 5061** per la linea ACE 12
- **45** pacchetti **HTTP** sulla **porta TCP 80** per la riga ACE 13
- **53** pacchetti **HTTPS** sulla **porta TCP 443** per la riga ACE 14
- **70** pacchetti **HTTP** sulla **porta TCP 8080** per la linea ACE 15
- **61** pacchetti **HTTPS** sulla **porta TCP 8443** per la riga ACE 16

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
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.18/16784
         dst inside:192.168.60.191/5060 by access-group "tACL-Policy"
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.200/16785
         dst inside:192.168.60.33/5060 by access-group "tACL-Policy"
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.99/16786
         dst inside:192.168.60.240/5061 by access-group "tACL-Policy"
  Apr 27 2011 00:03:41: %ASA-4-106023: Deny udp src outside:192.0.2.100/16787
         dst inside:192.168.60.115/5061 by access-group "tACL-Policy"
  Apr 27 2011 00:04:27: %ASA-4-106023: Deny tcp src outside:192.0.2.88/18683
         dst inside:192.168.60.38/5060 by access-group "tACL-Policy"
  Apr 27 2011 00:04:27: %ASA-4-106023: Deny tcp src outside:192.0.2.175/18684
         dst inside:192.168.60.250/5061 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** 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
  Apr 27 2011 00:03:42: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Apr 27 2011 00:03:43: %ASA-1-106021: Deny UDP reverse path check from
         192.168.60.1 to 192.168.60.100 on interface outside
  Apr 27 2011 00:03:43: %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.

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 alcune delle vulnerabilità descritte più avanti nel documento. Queste vulnerabilità possono essere rilevate dalle seguenti firme:

- 35846-0 - Cisco CUCM Remote Code Execution
- 35866-0 - Vulnerabilità Cisco CUCM SIP
- 35085-0 - Cisco Call Manager SQL Injection

35846-0 - Cisco CUCM Remote Code Execution

A partire dall'aggiornamento della firma S562 per i sensori che eseguono Cisco IPS versione 6.x e successive, queste vulnerabilità possono essere rilevate dalla firma 35846/0 (Nome firma: Cisco CUCM Remote Code Execution). La firma 35846/0 è abilitata per impostazione predefinita, attiva un evento di *alta* gravità, ha un indice di fedeltà della firma (SFR) di 95 ed è configurata con un'azione evento predefinita di **produce-alert**.

La firma 35846/0 viene attivata quando viene rilevato un singolo pacchetto inviato tramite la porta SIP 5060. L'attivazione di questa firma può indicare un potenziale sfruttamento di queste vulnerabilità.

35866-0 - Vulnerabilità Cisco CUCM SIP

A partire dall'aggiornamento della firma S562 per i sensori con Cisco IPS versione 6.x e successive, queste vulnerabilità possono essere rilevate dalla firma 35866/0 (nome firma: Cisco CUCM SIP Vulnerability). La firma 35866/0 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**.

La firma 3586/0 viene attivata quando viene rilevato un singolo pacchetto inviato tramite la porta SIP 5060. L'attivazione di questa firma può indicare un potenziale sfruttamento di queste vulnerabilità.

35085-0 - Cisco Call Manager SQL Injection

A partire dall'aggiornamento della firma S562 per i sensori con Cisco IPS versione 6.x e successive, queste vulnerabilità possono essere rilevate dalla firma 35085/0 (nome firma: Cisco Call Manager SQL Injection). La firma 35085/0 è abilitata per impostazione predefinita, attiva un evento di *alta* gravità, ha un indice di fedeltà della firma (SFR) di 85 ed è configurata con un'azione evento predefinita di **produce-alert**.

La firma 35085/0 viene attivata al rilevamento di un attacco SQL injection contro Call Manager di Cisco. 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: Simplify IPS Policy Management.

Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco

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

L'accessorio 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 35846/0 (nome firma: Cisco CUCM Remote Code Execution), la firma IPS 35866/0 (nome firma: Cisco CUCM SIP Vulnerability) e la firma IPS 35085/0 (nome firma: Cisco Call Manager SQL Injection). Una volta scaricato l'aggiornamento della firma dinamica S562, utilizzando la parola chiave **NR-35846/0** per la firma IPS 35846/0, la parola chiave **NR-35866/0** per la firma IPS 35866/0 o la parola chiave **NR-35085/0** per la firma IPS 35085/0 e un tipo di query **All Matching Events** sull'accessorio Cisco Security MARS fornirà un rapporto 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

IL PRESENTE DOCUMENTO VIENE FORNITO "COSÌ COM'È" E NON IMPLICA ALCUNA GARANZIA O CONCESSIONE, INCLUSE LE GARANZIA DI COMMERCIABILITÀ O IDONEITÀ PER UNO SCOPO SPECIFICO. L'UTILIZZO DA PARTE DELL'UTENTE DELLE INFORMAZIONI CONTENUTE NEL DOCUMENTO O NEI MATERIALI ACCESSIBILI DAL DOCUMENTO AVVIENE A PROPRIO RISCHIO. CISCO SI RISERVA IL DIRITTO DI MODIFICARE O AGGIORNARE IL PRESENTE DOCUMENTO IN QUALSIASI MOMENTO.

Cronologia delle revisioni

Revisione 1.1	27 APRILE 2011	Aggiornato per includere informazioni sulle firme IPS e Cisco Security MARS.
Revisione 1.0	27 APRILE 2011	Pubblicazione 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
- Presentazioni di Cisco Network Foundation Protection
- Un approccio orientato alla sicurezza per l'indirizzamento IP
- 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).