Identificazione e mitigazione dello sfruttamento delle vulnerabilità Denial of Service di Cisco Unified Communications Manager

Identificazione e mitigazione dello sfruttamento delle vulnerabilità Denial of Service di Cisco Unified Communications Manager

ID advisory: cisco-amb-20071017-cucm

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20071017-cucm

Revisione 1.2

Per la Pubblica Release 2007 Ottobre 17 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Questo bollettino sulla mitigazione applicata è un documento complementare all'advisory della sicurezza PSIRT *sulle vulnerabilità di negazione del servizio di Cisco Unified Communications Manager* e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

In alcune versioni di Cisco Unified Communications Manager (CUCM), in precedenza Cisco Unified CallManager, sono presenti più vulnerabilità. Queste vulnerabilità sono riepilogate nelle seguenti sottosezioni.

Session Initiation Protocol (SIP) INVITE UDP Denial of Service: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza interazione dell'utente. L'utilizzo riuscito di questa vulnerabilità può determinare una condizione DoS (Denial of Service). Ripetuti tentativi di

sfruttare questa vulnerabilità potrebbero causare una condizione DoS prolungata. Il vettore di attacco per lo sfruttamento è tramite pacchetti SIP che utilizzano la porta UDP 5060. Un utente non autorizzato potrebbe sfruttare questa vulnerabilità attraverso attacchi di spoofing. A questa vulnerabilità è stato assegnato il nome CVE CVE-2007-5537.

Overflow del servizio di localizzazione dei file TFTP (Trivial File Transfer Protocol) centralizzato: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza interazione dell'utente. L'utilizzo riuscito di questa vulnerabilità può consentire l'esecuzione arbitraria del codice e determinare una condizione DoS (Denial of Service). Ripetuti tentativi di sfruttare questa vulnerabilità potrebbero causare una condizione DoS prolungata. Il vettore di attacco per l'utilizzo è tramite pacchetti HTTP che utilizzano la porta TCP 6970. A questa vulnerabilità è stato assegnato il nome CVE CVE-2007-5538.

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-20071017-cucm.

Panoramica delle tecniche di mitigazione

I dispositivi Cisco forniscono diverse contromisure per le vulnerabilità di overflow del servizio SIP INVITE UDP denial of service e del servizio di localizzazione file TFTP centralizzato. 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.

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 le vulnerabilità descritte in questo documento.

Sul software Cisco IOS, la corretta implementazione e configurazione di Unicast RPF offre il mezzo più efficace di protezione dagli attacchi che usano pacchetti con indirizzi IP di origine oggetto di spoofing. È consigliabile distribuire RPF unicast il più vicino possibile a tutte le origini di traffico.

L'implementazione e la configurazione corrette di IPSG forniscono i mezzi più efficaci per la protezione dagli attacchi con indirizzi MAC di origine oggetto di spoofing.

Mezzi efficaci per prevenire gli attacchi possono essere forniti anche da Cisco ASA serie 5500 Adaptive Security Appliance, Cisco PIX serie 500 Security Appliance e Firewall Services Module (FWSM) per gli switch Cisco Catalyst serie 6500 e i router Cisco serie 7600, usando quanto segue:

- 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 le vulnerabilità descritte in questo documento.

Su Cisco ASA, PIX e FWSM, la corretta implementazione e configurazione di Unicast RPF offre i mezzi più efficaci di protezione dagli attacchi che usano pacchetti con indirizzi IP di origine oggetto di spoofing. È consigliabile distribuire RPF unicast il più vicino possibile a tutte le origini di traffico.

Cisco IOS NetFlow può fornire visibilità su questi tentativi di sfruttamento utilizzando i record di flusso.

Il software Cisco IOS, Cisco ASA, le appliance di sicurezza Cisco PIX e i firewall FWSM possono fornire visibilità attraverso i messaggi syslog e i valori dei contatori visualizzati nell'output dei comandi **show**.

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

L'appliance Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) può inoltre fornire visibilità tramite query e report di eventi.

Gestione dei rischi

Le organizzazioni dovrebbero 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 nei progetti di sicurezza delle informazioni possono aiutare le organizzazioni a sviluppare processi di valutazione della sicurezza e di risposta ripetibili.

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, PIX 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, è necessario che gli amministratori distribuiscano 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.

Il criterio ACL nega l'invio ai dispositivi interessati di pacchetti SIP non autorizzati sulla porta UDP 5060 e pacchetti HTTP sulla porta TCP 6970. Nell'esempio seguente, 192.168.1.0/24 è lo spazio degli indirizzi IP di rete utilizzato dai dispositivi interessati e l'host in 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.

Ulteriori informazioni sugli ACL sono disponibili in Access Control Lists: Filtering at Your Edge (Liste di controllo dell'accesso in transito: filtraggio sul perimetro della rete).

```
! !--- Include any explicit permit statements for trusted sources !--- that require
access on the vulnerable ports ! access-list 150 permit udp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 5060 access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 6970 ! !--- The following vulnerability-specific access
control entries !--- (ACEs) can aid in identification of attacks ! access-list 150
deny udp any 192.168.1.0 0.0.0.255 eq 5060 access-list 150 deny tcp any 192.168.1.0
0.0.0.255 eq 6970 ! !--- 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 ! 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*.

Inoltro percorso inverso unicast

La vulnerabilità del denial of service UDP SIP INVITE può essere sfruttata da pacchetti IP oggetto di spoofing. La corretta distribuzione e configurazione di Unicast Reverse Path Forwarding (Unicast RPF) può fornire meccanismi di protezione per lo spoofing correlato alla vulnerabilità SIP INVITE UDP Denial of Service.

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 proteggere al 100% dallo 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 l'interruzione del 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 libera.

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. L'installazione e la configurazione corrette di IPSG, abbinate a RPF unicast in modalità rigorosa, possono fornire i mezzi più efficaci per la protezione da spoofing al fine di ridurre la vulnerabilità SIP INVITE UDP Denial of Service.

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 sulla porta UDP 5060 e di pacchetti HTTP sulla porta TCP 6970 che sono stati filtrati. Gli amministratori devono esaminare i 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 udp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 5060
    20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 6970
    30 deny udp any 192.168.1.0 0.0.0.255 eq 5060 (12 matches)
    40 deny tcp any 192.168.1.0 0.0.0.255 eq 6970 (26 matches)
    50 deny ip any any
router#
```

Nell'esempio precedente, l'elenco degli accessi 150 ha scartato 12 pacchetti SIP sulla porta UDP 5060 per i pacchetti **HTTP** con ID sequenza ACE 30 e **26** sulla porta **TCP 6970** per l'ID sequenza ACE 40.

Identificazione: Registrazione elenco accessi

L'opzione **log** o **log-input** access control list (ACL) causa la registrazione di 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 della lista di controllo degli accessi può richiedere un utilizzo intensivo della CPU e deve essere utilizzata con estrema cautela. I fattori che determinano l'impatto della registrazione ACL sulla CPU sono la generazione di log, la trasmissione di log e la commutazione di processo per inoltrare i pacchetti che corrispondono alle voci ACE abilitate per il log.

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. 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.

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 ip interface, **show cef drop**, **show cef interface** *type slot/port* **internal** e **show ip traffic** per identificare il numero di pacchetti ignorati dal protocollo RPF unicast.

Nota: il *comando* **show** | **begin** *regexp* and **show**, *comando* | **include** *regexp* i modificatori del comando vengono utilizzati negli esempi seguenti per ridurre al minimo la quantità di output che gli amministratori devono analizzare per visualizzare le informazioni desiderate. Per ulteriori informazioni sui modificatori di comando, consultare le sezioni "show command" della guida di riferimento dei comandi di Cisco IOS Configuration Fundamentals.

Nota: il comando **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
    !--- CLI Output Truncated
   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
IPv6 CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route    No_adj
RP             0           0           0           3         0
router#
```

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
      --      CLI Output Truncated       --
  ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0, allow self-ping
router#
```

```
router#show ip traffic

IP statistics:
  Rcvd:  68051015 total, 2397325 local destination
         43999 format errors, 0 checksum errors, 33 bad hop count
         2 unknown protocol, 929 not a gateway
         21 security failures, 190123 bad options, 542768 with options
```

```
  Opts:  352227 end, 452 nop, 36 basic security, 1 loose source route
         45 timestamp, 59 extended security, 41 record route
         53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump
         361634 other
  Frags: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 64666 received, 0 sent
  Mcast: 1589885 received, 2405454 sent
  Sent:  3001564 generated, 65359134 forwarded

  Drop:  4256 encapsulation failed, 0 unresolved, 0 no adjacency
         18 no route, 18 unicast RPF, 0 forced drop
         0 options denied
  Drop:  0 packets with source IP address zero
  Drop:  0 packets with internal loop back IP address
    !--- CLI Output Truncated router#
```

Negli esempi precedenti, Unicast RPF ha scartato **18 pacchetti IP** ricevuti a livello globale su tutte le interfacce con Unicast RPF configurato a causa dell'impossibilità di verificare l'indirizzo di origine dei pacchetti IP nella base di informazioni di inoltro di Cisco Express.

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 possono essere tentativi di sfruttare le vulnerabilità descritte in questo documento. Gli amministratori devono analizzare i flussi per stabilire se sono tentativi di sfruttare queste vulnerabilità o se si tratta di flussi di traffico legittimi.

```
router#show ip cache flow

IP packet size distribution (1103375 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .004 .434 .081 .017 .011 .033 .001 .010 .001 .000 .009 .000 .001 .001 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .002 .380 .002 .004 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
  12 active, 65524 inactive, 54766 added
  3098504 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds
  IP Sub Flow Cache, 402120 bytes
  24 active, 16360 inactive, 109532 added, 54766 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         869      0.0        38    41      0.1      20.6      43.2
TCP-FTP             31      0.0        16    59      0.0       6.7      28.0
TCP-WWW           2996      0.0        12   231      0.1       8.2      11.4
TCP-other        24997      0.0        38   288      3.3      25.5      21.1
UDP-DNS            361      0.0         2    49      0.0       0.9      60.4
UDP-NTP          13982      0.0         1    76      0.0       0.8      60.5
UDP-other        10136      0.0         3   159      0.1      25.3      48.6
ICMP               556      0.0         7    68      0.0      51.4      39.6
Total:           53928      0.1        20   270      3.7      18.1      36.8
```

```
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.208.64  Gi0/1         192.168.1.21    11 13C4 13C4  1458
Gi0/0         192.16820.67    Gi0/1         192.168.150.60  06 0707 0016    80
Gi0/0         192.168.208.63  Gi0/1         192.168.1.21    06 84F2 1B3A     4
Gi0/0         192.168.14.132  Gi0/1         192.168.150.60  06 1A29 90AB     2
Gi0/0         192.168.115.113 Gi0/1         192.168.128.21  06 09BD 0017     2
Gi0/0         192.168.115.113 Local         192.168.128.20  06 0981 0017    31
Gi0/0         192.168.115.113 Gi0/1         192.168.130.41  06 0B83 01BB    30
Gi0/0         192.168.226.1   Gi0/1         192.168.206.5   11 007B 007B     1
Gi0/0         192.168.226.1   Local         192.168.128.20  11 007B 007B     1
Gi0/0         192.168.226.1   Gi0/1         192.168.128.21  11 007B 007B     1
router#
```

Nell'esempio precedente, sono presenti più flussi per i pacchetti SIP sulla porta UDP 5060 **(valore esadecimale 13C4)** e per i pacchetti HTTP sulla porta TCP 6970 **(valore esadecimale 1B3A)**. I pacchetti UDP in questi flussi possono essere oggetto di spoofing e possono indicare un tentativo di sfruttare le vulnerabilità descritte in questo documento. Gli amministratori devono confrontare questi flussi con l'utilizzo di base per i pacchetti SIP sulla porta UDP 5060 e sulla porta TCP 6970 e analizzare i flussi per determinare se provengono da host o reti non attendibili.

Per visualizzare solo i flussi di traffico per i pacchetti SIP sulla porta UDP 5060 **(valore esadecimale 13C4)**, usare il comando **show ip cache flow | include SrcIf|_11_.*13C4** visualizzerà i record NetFlow correlati, come mostrato di seguito:

```
router#show ip cache flow | include SrcIf|_11_.*13C4
SrcIf         SrcIPaddress     DstIf DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.208.64   Gi0/1 192.168.1.21    11 13C4 13C4  1458
router#
```

Per visualizzare solo i flussi di traffico per la porta TCP 6970 **(valore esadecimale 1B3A)**, eseguire il comando **show ip cache flow | include SrcIf|_06_.*1B3A** visualizzerà i record NetFlow correlati, come mostrato di seguito:

```
router#show ip cache flow | include SrcIf|_06_.*1B3A
SrcIf         SrcIPaddress     DstIf DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.208.63   Gi0/1 192.168.1.21    06 84F2 1B3A     4
router#
```

Cisco ASA, PIX 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, gli amministratori devono 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.

Il criterio ACL nega l'invio ai dispositivi interessati di pacchetti SIP non autorizzati sulla porta UDP 5060 e pacchetti HTTP sulla porta TCP 6970. Nell'esempio seguente, 192.168.1.0/24 è lo spazio degli indirizzi IP di rete utilizzato dai dispositivi interessati e l'host in 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.

Ulteriori informazioni sugli ACL sono disponibili in Access Control Lists: Filtering at Your Edge (Liste di controllo dell'accesso in transito: filtraggio sul perimetro della rete).

```
! !--- Include any explicit permit statements for trusted sources !--- that require
access on the vulnerable ports ! access-list Transit-ACL-Policy extended permit udp
host 192.168.100.1 192.168.1.0 255.255.255.0 eq 5060 access-list Transit-ACL-Policy
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq 6970 ! !--- The
following vulnerability-specific access control entries !--- (ACEs) can aid in
identification of attacks ! access-list Transit-ACL-Policy extended deny udp any
192.168.1.0 255.255.255.0 eq 5060 access-list Transit-ACL-Policy extended deny tcp
any 192.168.1.0 255.255.255.0 eq 6970 ! !--- 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 ! access-list Transit-ACL-Policy extended
deny ip any any ! !--- Apply tACL to interfaces in the ingress direction ! access-
group Transit-ACL-Policy in interface outside
```

Attenuazione: protezione da spoofing con inoltro percorso inverso unicast

La vulnerabilità del denial of service UDP SIP INVITE può essere sfruttata da pacchetti IP oggetto di spoofing. La corretta distribuzione e configurazione di Unicast Reverse Path Forwarding (Unicast RPF) può fornire meccanismi di protezione per lo spoofing correlato alla vulnerabilità SIP INVITE UDP Denial of Service.

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 proteggere al 100% dallo 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 sulla porta UDP 5060 e di pacchetti HTTP sulla porta TCP 6970 che sono stati filtrati. Gli amministratori devono esaminare i pacchetti filtrati per determinare se sono tentativi di sfruttare queste vulnerabilità. Di seguito è riportato un output di esempio per **show access-list Transit-ACL-Policy**:

```
firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 5 elements
access-list Transit-ACL-Policy line 1 extended permit udp host 192.168.100.1
192.168.1.0 255.255.255.0 eq sip
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1
192.168.1.0 255.255.255.0 eq 6970
access-list Transit-ACL-Policy line 3 extended deny udp any 192.168.1.0 255.255.255.0
eq sip (hitcnt=4378)
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0 255.255.255.0
eq 6970
```

```
access-list Transit-ACL-Policy line 5 extended deny ip any any
firewall#
```

Nell'esempio precedente, l'elenco degli accessi *Transit-ACL-Policy* ha scartato **4378** pacchetti SIP sulla porta UDP **5060** ricevuti da un host o da una rete non attendibile. Inoltre, il messaggio syslog *106023* può fornire informazioni preziose, tra cui l'indirizzo IP di origine e di destinazione, i numeri di porta di origine e di destinazione e il protocollo IP per il pacchetto rifiutato.

Identificazione: Messaggi syslog lista 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 su questo messaggio syslog, consultare il log Message del sistema Cisco Security Appliance - 106023.

Per informazioni sulla configurazione del syslog per Cisco ASA serie 5500 Adaptive Security Appliance o Cisco PIX serie 500 Security Appliance, consultare il documento sulla configurazione della registrazione su Cisco Security Appliance. 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 sulla configurazione del monitoraggio e della registrazione sul modulo FWSM Cisco.

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 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 Utilizzo dell'interfaccia della riga di comando.

```
firewall#show logging | grep 106021
Sep 20 2007 10:07:01: %ASA-4-106023: Deny udp src outside:192.168.2.18/5210 dst
   inside:192.168.1.191/5060 by access-group "Transit-ACL-Policy"
Sep 20 2007 10:07:01: %ASA-4-106023: Deny tcp src outside:192.168.3.200/3521 dst
   inside:192.168.1.33/6970 by access-group "Transit-ACL-Policy"
firewall#
```

Nell'esempio precedente, l'elenco degli accessi *Transit-ACL-Policy* ha scartato **4378** pacchetti SIP sulla porta UDP **5060** ricevuti da un host o da una rete non attendibile. Inoltre, il messaggio syslog *106023* può fornire informazioni preziose, tra cui l'indirizzo IP di origine e di destinazione, i numeri di porta di origine e di destinazione e il protocollo IP per il pacchetto rifiutato.

Per ulteriori informazioni sui messaggi syslog per appliance di sicurezza ASA e PIX, consultare il documento Cisco Security Appliance System Log Messages. Per ulteriori informazioni sui messaggi syslog per FWSM, consultare i messaggi di configurazione della registrazione del modulo dei servizi firewall del router Catalyst serie 6500 e del registro di sistema del router Cisco serie 7600.

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 su questo messaggio syslog, consultare il log Message del sistema Cisco Security Appliance - 106021.

Per informazioni sulla configurazione del syslog per Cisco ASA serie 5500 Adaptive Security

Appliance o Cisco PIX serie 500 Security Appliance, consultare il documento sulla configurazione della registrazione su Cisco Security Appliance. 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 sulla configurazione del monitoraggio e della registrazione sul modulo FWSM Cisco.

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 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 Utilizzo dell'interfaccia della riga di comando.

```
firewall#show logging | grep 106021
Sep 20 2007 10:07:01: %ASA-1-106021: Deny UDP reverse path check from 192.168.0.1 to
192.168.0.100 on interface outside
Sep 20 2007 10:07:01: %ASA-1-106021: Deny UDP reverse path check from 192.168.0.1 to
192.168.0.100 on interface outside
Sep 20 2007 10:07:01: %ASA-1-106021: Deny TCP reverse path check from 192.168.0.1 to
192.168.0.100 on interface outside
firewall#
```

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

```
firewall#show asp drop

Frame drop:
  Reverse-path verify failed                          11
  Flow is denied by configured rule                  855
  Expired flow                                         1
  Interface is down                                    2

Flow drop:

firewall#
```

Nell'esempio precedente, Unicast RPF ha scartato **11 pacchetti IP** ricevuti su interfacce con Unicast RPF configurato.

Per ulteriori informazioni sulla configurazione e l'utilizzo di RPF unicast, consultare 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 dei servizi di Cisco Intrusion Prevention System (IPS) per rilevare le minacce e contribuire a prevenire i tentativi di sfruttare le vulnerabilità descritte più avanti nel documento. Queste vulnerabilità possono essere rilevate dalle seguenti firme:

- 5912/0 - CUCM SIP INVITE UDP Denial of Service
- 5910/0 - Overflow buffer del servizio di localizzazione file TFTP centralizzato CUCM

5912/00 - CUCM SIP INVITE UDP Denial of Service.

A partire dall'aggiornamento della firma S307 per i sensori con Cisco IPS versione 6.x o 5.x, le vulnerabilità descritte in questo documento possono essere rilevate dalla firma 6912/0 (nome firma: UCCM Centralized TFTP File Locator Service Buffer Overflow. La firma 5912/0 è abilitata per impostazione predefinita, attiva un evento di gravità *Medio*, ha un indice di fedeltà della firma (SFR) di 80 ed è configurata con un'azione evento predefinita **Genera avviso**. La firma 5912/0 viene attivata quando vengono rilevati più pacchetti inviati tramite la porta UDP 5060. L'attivazione di questa firma può indicare un potenziale utilizzo delle vulnerabilità descritte nel presente documento.

5910/0 - Overflow del buffer del servizio di localizzazione file TFTP centralizzato CUCM.

A partire dall'aggiornamento della firma S307 per i sensori con Cisco IPS versione 6.x o 5.x, le vulnerabilità descritte in questo documento possono essere rilevate dalla firma 5910/0 (nome firma: UCM Centralized TFTP File Locator Service Buffer Overflow). La firma 5910/0 è abilitata per impostazione predefinita, attiva un evento di gravità *Medio*, ha un SFR di 75 ed è configurata con un'azione evento predefinita **Avviso produzione**. La firma 5910/0 viene attivata quando vengono rilevati più pacchetti inviati tramite la porta TCP 6970. L'attivazione di questa firma può indicare un potenziale utilizzo delle vulnerabilità descritte nel presente documento.

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.

Per sfruttare questa vulnerabilità è necessario stabilire l'handshake TCP a tre vie, che riduce la possibilità di attacchi riusciti utilizzando indirizzi IP spoofed, nonché eventi falsi positivi per la firma 5910/0.

Poiché gli exploit basati su UDP possono essere facilmente oggetto di spoofing, un attacco che contiene indirizzi oggetto di spoofing può causare un'azione evento configurata per negare inavvertitamente il traffico proveniente da fonti attendibili. Le azioni evento che eseguono il blocco tramite ACL o il comando shun vengono in genere configurate sui sensori distribuiti in modalità promiscua.

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 installati in modalità di protezione inline fornisce la prevenzione delle minacce contro gli attacchi che tentano di sfruttare queste vulnerabilità. La prevenzione delle minacce viene ottenuta tramite un override predefinito che esegue un'azione evento **Deny Connection Inline** e **Produce un avviso** per le firme attivate con *riskRatingValue* maggiore di 90. Ulteriori informazioni sul rating del rischio e sul calcolo del suo valore sono disponibili in Spiegazione della classificazione del rischio di Cisco IPS.

I sensori Cisco IPS 5.x installati in modalità di protezione inline devono avere un'azione evento configurata per singola firma. In alternativa, gli amministratori possono configurare una sostituzione in grado di eseguire un'azione evento per qualsiasi firma attivata e calcolata come minaccia ad alto rischio. L'utilizzo dell'azione evento **Deny Connection Inline** e **Produce Alert** sui sensori installati in modalità di protezione inline fornisce la prevenzione più efficace degli attacchi.

Identificazione: eventi firma IPS

5912/00 - CUCM SIP INVITE UDP Denial of Service.

```
IPS# show events alert
evIdsAlert: eventId=1184086129278931859 severity=medium vendor=Cisco
  originator:
    hostId: R4-IPS4240a
    appName: sensorApp
    appInstanceId: 402
  time: 2007/10/17 17:14:21 2007/10/17 12:14:21 CDT
  signature: description=CUCM SIP INVITE UDP Denial of Service id=5912 version=S307
    subsigId: 0
    sigDetails: CUCM SIP INVITE UDP Denial of Service
    marsCategory: DoS/Network/UDP
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.208.64
      port: 5060
    target:
      addr: locality=OUT 192.168.132.44
      port: 5060
      os: idSource=learned relevance=relevant type=linux
   triggerPacket:
 !--- Packet details removed riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium 60 threatRatingValue: 60 interface: ge0_0 protocol: udp
```

5910/0 - Overflow del buffer del servizio di localizzazione file TFTP centralizzato CUCM.

```
IPS# show events alert
evIdsAlert: eventId=1184086129278930978 severity=medium vendor=Cisco
  originator:
    hostId: IPS
    appName: sensorApp
    appInstanceId: 402
  time: 2007/10/17 17:00:57 2007/10/17 12:00:57 CDT
  signature: description=CUCM Centralized TFTP File Locator Service Buffer Overflow
id=5910 version=S307
    subsigId: 0
    sigDetails: Buffer overflow in TFTP over HTTP
    marsCategory: Penetrate/BufferOverflow/Web
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.208.63
      port: 32806
    target:
      addr: locality=OUT 192.168.132.44
      port: 6970
      os: idSource=learned relevance=relevant type=linux
    context:
      fromAttacker:
!--- Packet Details Removed riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium watchlist=25 81 threatRatingValue: 81 interface: ge0_0
protocol: tcp
```

Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco

Identificazione: tipo di query e parola chiave Cisco Security Monitoring, Analysis, and Response

System

L'appliance Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) può eseguire query sugli eventi per rilevare le vulnerabilità di negazione del servizio CUCM utilizzando un tipo di query e una parola chiave. Utilizzando una parola chiave di NR-5912/0 per la firma IPS **5912/0**, che può rilevare la vulnerabilità SIP INVITE UDP denial of service; parola chiave di **NR-5910/0** per la firma IPS **5910/0**, che può rilevare la vulnerabilità di overflow del servizio TFTP centralizzato di localizzazione file; e un tipo di query di **Tutti i messaggi raw di eventi corrispondenti** sull'appliance Cisco Security MARS, sarà disponibile un report che elenca gli eventi creati dalla firma IPS 599 12/0 o 5910/0.

La schermata seguente mostra i valori utilizzati per eseguire query sugli eventi creati dalla firma IPS 5912/0 (nome firma: CUCM SIP INVITE UDP Denial of Service) o dalla firma IPS 5910/0 (nome firma: UCCM Centralized TFTP File Locator Service Buffer Overflow).

La schermata seguente mostra i risultati della query per **NR-5912/0 o NR-5910/0** creata dall'accessorio Cisco Security MARS utilizzando una query con tipo di query e parola chiave regex.

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 1.2	22 ottobre 2007	Includi nomi CVE assegnati
Revisione 1.1	17 ottobre 2007	Includi informazioni su pacchetto di firma IPS S307
Revisione 1.0	17 ottobre 2007	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
- Protezione del core: Access Control List di protezione dell'infrastruttura

- Access Control List transit: filtraggio sul perimetro della rete
- Informazioni sulla registrazione della lista di controllo dell'accesso
- Informazioni sull'inoltro di percorsi inverso unicast
- Cisco IOS NetFlow - Home Page su Cisco.com
- White paper su Cisco IOS NetFlow
- Prodotti Cisco Firewall - Home Page su Cisco.com
- Modalità Loose di inoltro percorso inverso unicast
- Vulnerabilità ed esposizioni comuni (CVE)
- Cisco 6.x Intrusion Prevention System
- Spiegazione della classificazione del rischio Cisco IPS
- Download per le firme Cisco IPS 6.x
- Firme Cisco IPS per versione (solo utenti registrati)
- Firme Cisco IPS per Signature ID (solo utenti registrati)
- Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco

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).