Identificazione e mitigazione dello sfruttamento delle molteplici vulnerabilità di Cisco Unified Communications Manager e del server di presenza

Identificazione e mitigazione dello sfruttamento delle molteplici vulnerabilità di Cisco Unified Communications Manager e del server di presenza

Codice identificativo: cisco-amb-20070711-cucm

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070711-cucm

Revisione 1.0

Per la Pubblica Release 2007 Luglio 11 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Il presente Bollettino sulla mitigazione applicata è un documento complementare ai seguenti consigli di sicurezza PSIRT: *Vulnerabilità di overflow di Cisco Unified Communications Manager* e *Vulnerabilità di accesso non autorizzato di Cisco Unified Communications Manager e di Presence Server* e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

Cisco Unified Communications Manager e Cisco Unified Presence Server presentano diverse vulnerabilità. Queste vulnerabilità sono riepilogate nelle seguenti sottosezioni:

Overflow del servizio del provider dell'elenco di certificati attendibili: 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 di codice o causare una condizione di Denial of Service (DoS). Il vettore di attacco è costituito dai pacchetti inviati alla porta del servizio del provider dell'elenco di certificati attendibili (CTL). La porta predefinita è la porta TCP 244. Gli amministratori possono verificare la porta utilizzata dal servizio del provider CTL consultando l'interfaccia utente grafica di Cisco Unified Communications Manager: selezionare **Sistema > Parametri servizio**. Dall'elenco a discesa Server, scegliere il server. Quindi, scegliere **Cisco CTL Provider (Inactive)** o **Cisco CTL Provider (Active)** dall'elenco a discesa Servizio. Il termine *(Inattivo)* o *(Attivo)* aggiunto al nome del servizio in questo elenco indica se il servizio è abilitato. Dopo aver scelto il servizio, il parametro Port Number è visibile nell'area sotto gli elenchi a discesa Server e Servizio. Il valore di questo parametro indica la porta utilizzata per il servizio quando è attivo. Al momento della pubblicazione non era presente alcun ID CVE associato a questa vulnerabilità.

Informazioni sul software vulnerabile, non interessato e fisso sono disponibili in PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm.

Overflow dell'heap dell'agente di raccolta dati del server delle informazioni in tempo reale: 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 di codice o causare una condizione di Denial of Service (DoS). Il vettore di attacco è costituito dai pacchetti inviati alla porta dell'agente di raccolta dati di Real-Time Information Server (RIS). La porta predefinita è TCP 2556. Gli amministratori possono verificare la porta utilizzata dal servizio Agente di raccolta dati RIS consultando l'interfaccia utente grafica di Cisco Unified Communications Manager: Scegliere **Sistema > Parametri servizio**. Dall'elenco a discesa Server, scegliere il server. Quindi scegliere **Cisco RIS Data Collector (Inactive)** o **Cisco RIS Data Collector (Active)** dall'elenco a discesa Servizio. Il termine *(Inattivo)* o *(Attivo)* aggiunto al nome del servizio in questo elenco indica se il servizio è abilitato. Dopo aver scelto il servizio, il parametro Porta TCP del cluster RIS sarà visibile nell'area Parametri a livello di cluster. Il valore di questo parametro indica la porta utilizzata per il servizio quando è attivo. Al momento della pubblicazione non era presente alcun ID CVE associato a questa vulnerabilità.

Informazioni sul software vulnerabile, non interessato e fisso sono disponibili in PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-cucm.

Gli amministratori non autorizzati possono attivare/terminare i servizi di sistema di Cisco Unified Communications Manager/Cisco Unified Presence Server: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza interazione dell'utente. Un utilizzo corretto può consentire a un amministratore di Cisco Unified Communications Manager/Cisco Unified Presence Server non autorizzato di attivare o terminare i servizi di sistema in un ambiente cluster. Ciò può interrompere o arrestare i servizi vocali critici. Il vettore di attacco è il protocollo SSL che utilizza i pacchetti della porta TCP 8443. Per ulteriori informazioni sulle porte usate dal software interessato, vedere Uso delle porte TCP e UDP di Cisco CallManager. Al momento della pubblicazione non era presente alcun ID CVE associato a questa vulnerabilità.

Informazioni sul software vulnerabile, non interessato e fisso sono disponibili in PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-voip.

Gli amministratori non autorizzati possono visualizzare le impostazioni SNMP di Cisco Unified

Communications Manager/Cisco Unified Presence Server: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza interazione dell'utente. Se l'utilizzo riesce, è possibile che un amministratore non autorizzato possa esplorare la visualizzazione delle impostazioni SNMP su un'interfaccia di gestione di un nodo cluster Cisco Unified Communications Manager/Cisco Unified Presence Server. Il vettore di attacco è il protocollo SSL che utilizza i pacchetti della porta TCP 8443. Per ulteriori informazioni sulle porte usate dal software interessato, vedere Uso delle porte TCP e UDP di Cisco CallManager. Al momento della pubblicazione non era presente alcun ID CVE associato a questa vulnerabilità.

Informazioni sul software vulnerabile, non interessato e fisso sono disponibili in PSIRT Security Advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070711-voip.

Panoramica delle tecniche di mitigazione

I dispositivi Cisco forniscono diverse contromisure per le vulnerabilità descritte in questo documento. Si consiglia agli amministratori di considerare molti di 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 essere uno strumento efficace per prevenire gli attacchi tramite gli Access Control List (tACL) di transito.

Un'efficace prevenzione degli attacchi può essere fornita anche da Cisco ASA serie 5500 Adaptive Security Appliance, Cisco PIX serie 500 Security Appliance e dal Firewall Services Module (FWSM) per gli switch Cisco Catalyst serie 6500 e i router Cisco serie 7600 con Access Control List (tACL) di transito.

Questi meccanismi di protezione filtrano ed eliminano i pacchetti che tentano di sfruttare le vulnerabilità descritte in questo documento.

Cisco IOS NetFlow può fornire visibilità sui tentativi di sfruttamento tramite 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**.

Gestione dei rischi

Le organizzazioni dovrebbero seguire il loro processo 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

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 non autorizzati per il servizio Provider TCP sulla porta TCP 2444, per l'agente di raccolta dati RIS sulla porta TCP 2556 e per i servizi di sistema Cisco Unified Communications Manager/Cisco Unified Presence Server sulla porta TCP 8443. 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 port(s) ! access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 2444 access-list 150 permit tcp host 192.168.100.1
192.168.1.0 0.0.0.255 eq 2556 access-list 150 permit tcp host 192.168.100.1
192.168.1.0 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 192.168.1.0 0.0.0.255 eq 2444 access-list 150 deny tcp any 192.168.1.0
0.0.0.255 eq 2556 access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq 8443 ! !--
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 interface(s) 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. Ciò potrebbe avere l'effetto indesiderato di aumentare l'utilizzo della CPU perché il dispositivo deve generare questi messaggi ICMP "destinazione irraggiungibile". 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 icmp 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*.

Identificazione: Access Control List transit

Dopo che l'amministratore ha applicato il tACL a un'interfaccia, il comando **show ip access-lists** restituisce il numero di pacchetti del servizio Provider TCP sulle porte TCP 2444, di pacchetti dell'agente di raccolta dati RIS sulla porta TCP 2556 e di pacchetti del servizio di sistema CUCM/CUPS sulla porta TCP 8443 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 tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2444 (2 matches)
    20 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 2556 (3 matches)
    30 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq 8443 (3 matches)
    40 deny tcp any 192.168.1.0 0.0.0.255 eq 2444 (3 matches)
    50 deny tcp any 192.168.1.0 0.0.0.255 eq 2556 (4 matches)
    60 deny tcp any 192.168.1.0 0.0.0.255 eq 8443 (5 matches)
    70 deny ip any any
router#
```

Nell'esempio precedente, l'elenco degli accessi 150 ha scartato **3 pacchetti sulla porta TCP 2444** per l'ID sequenza ACE 40, **4 pacchetti sulla porta TCP 2556** per l'ID sequenza ACE 50 e **5 pacchetti sulla porta TCP 8443** per l'ID sequenza ACE 60.

Identificazione: Registrazione elenco accessi

L'opzione **log** o **log-input** 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. L'impatto sulla CPU del log ACL è determinato da due fattori: la commutazione di contesto risultante dalla corrispondenza di pacchetti che corrispondono ad ACE abilitati per il log e la generazione e la trasmissione del log.

L'impatto sulla CPU causato dalla registrazione ACL può essere risolto tramite hardware sugli switch Catalyst serie 6500 e sui router Cisco serie 7600 con Supervisor 720 e Supervisor 32 utilizzando la registrazione 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 sull'intelligence applicata all'indirizzo http://www.cisco.com/web/about/security/intelligence/acl-logging.html.

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 potenziali 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 (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

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

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet    11393421      2.8         1    48      3.1       0.0       1.4
TCP-FTP           236       0.0        12    66      0.0       1.8       4.8
TCP-FTPD           21       0.0     13726  1294      0.0      18.4       4.1
TCP-WWW         22282       0.0        21  1020      0.1       4.1       7.3
TCP-X             719       0.0         1    40      0.0       0.0       1.3
TCP-BGP             1       0.0         1    40      0.0       0.0      15.0
TCP-Frag        70399       0.0         1   688      0.0       0.0      22.7
TCP-other     47861004     11.8         1   211     18.9       0.0       1.3
UDP-DNS           582       0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957     14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.100.201 Gi0/1         192.168.1.102   06 0984 098C     1
Gi0/0         192.168.100.5   Gi0/1         192.168.1.158   06 0911 09FC     3
Gi0/0         192.168.105.60  Gi0/1         192.89.1.226    06 0016 12CA     1
Gi0/0         192.168.105.97  Gi0/1         192.168.1.28    06 0B3E 098C     5
Gi0/0         192.168.105.197 Gi0/1         192.168.1.248   06 0B3E 20FB     7
Gi0/0         192.168.1.17    Gi0/1         192.168.1.97    11 0B89 00A1     1
Gi0/0         192.168.105.7   Gi0/1         192.168.1.8     06 0B3E 20FB     4
Gi0/1         10.88.226.1     Gi0/0         192.168.202.22  11 007B 007B     1
Gi0/0         192.168.12.185  Gi0/1         192.168.1.239   06 0E8A 09FC     1
Gi0/1         10.89.16.226    Gi0/0         192.168.150.60  06 12CA 0901     1
router#
```

Nell'esempio precedente vengono rilevati diversi flussi per il servizio Provider CTL sulla **porta TCP 2444 (valore esadecimale 098C)**, per l'agente di raccolta dati RIS sulla **porta TCP 2556 (valore esadecimale 09FC)** e per il servizio di sistema Cisco Unified Communications Manager/Cisco Unified Presence Server sulla **porta TCP 8443 (valore esadecimale 20FB)**. Gli amministratori devono confrontare questi flussi con l'utilizzo di base per il traffico inviato sulle porte TCP 2444, 2556 e 8443 e analizzare i flussi per determinare se provengono da host o reti non attendibili.

Per visualizzare solo i flussi di traffico per i pacchetti sulla porta TCP 2444 (valore esadecimale 098C), i pacchetti sulla porta TCP 2556 (valore esadecimale 09FC) o i pacchetti sulla porta TCP 8443 (valore esadecimale 20FB), eseguire il comando **show ip cache flow | include SrcIf|_06_.*(098C|09FC|20FB)** visualizzerà i record NetFlow correlati, come mostrato di seguito:

```
router#show ip cache flow | include SrcIf|_06_.*(098C|09FC|20FB)
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.100.110  Gi0/1         192.168.1.163   06 0E2A 098C     6
Gi0/0         192.168.105.230  Gi0/1         192.168.1.20    06 0C09 098C     1
Gi0/0         192.168.101.131  Gi0/1         192.168.1.245   06 0B66 20FB    18
Gi0/0         192.168.100.7    Gi0/1         192.168.1.162   06 0D14 09FC     1
Gi0/0         192.168.100.86   Gi0/1         192.168.1.27    06 0B7B 09FC     2
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 i pacchetti non autorizzati del servizio Provider TCP sulla porta TCP 2444, i pacchetti dell'agente di raccolta dati RIS sulla porta TCP 2556 e i pacchetti del servizio di sistema Cisco Unified Communications Manager/Cisco Unified Presence Server sulla porta TCP 8443 inviati ai dispositivi interessati. 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 port(s) ! access-list Transit-ACL-Policy extended permit tcp
host 192.168.100.1 192.168.1.0 255.255.255.0 eq 2444 access-list Transit-ACL-Policy
extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0 eq 2556 access-list
Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.1.0 255.255.255.0
eq 8443 ! !-- The following vulnerability-specific access control entries !-- (ACEs)
can aid in identification of attacks ! access-list Transit-ACL-Policy extended deny
tcp any 192.168.1.0 255.255.255.0 eq 2444 access-list Transit-ACL-Policy extended
deny tcp any 192.168.1.0 255.255.255.0 eq 2556 access-list Transit-ACL-Policy
extended deny tcp any 192.168.1.0 255.255.255.0 eq 8443 ! !-- 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 interface(s) in the ingress
direction ! access-group Transit-ACL-Policy in interface outside !
```

Identificazione: Access Control List transit

Dopo aver applicato l'ACL a un'interfaccia, gli amministratori possono utilizzare il comando **show access-list** per identificare il numero di pacchetti del servizio Provider TCP sulla porta TCP 2444, di pacchetti dell'agente di raccolta dati RIS sulla porta TCP 2556 e di pacchetti del servizio di sistema Cisco Unified Communications Manager/Cisco Unified Presence Server sulla porta TCP 8443 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; 7 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 2444 (hitcnt=2) 0xaca1615c
access-list Transit-ACL-Policy line 2 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 2556 (hitcnt=4) 0x991fbe7d
access-list Transit-ACL-Policy line 3 extended permit tcp host 192.168.100.1
            192.168.1.0 255.255.255.0 eq 8443 (hitcnt=3) 0xd2687825
access-list Transit-ACL-Policy line 4 extended deny tcp any 192.168.1.0255.255.255.0
            eq 2444 (hitcnt=19) 0xc81a715d
access-list Transit-ACL-Policy line 5 extended deny tcp any 192.168.1.0255.255.255.0
            eq 2556 (hitcnt=11) 0x67db99e7
access-list Transit-ACL-Policy line 6 extended deny tcp any 192.168.1.0255.255.255.0
            eq 8443 (hitcnt=7) 0xb322498f
access-list Transit-ACL-Policy line 7 extended deny ip any any(hitcnt=0) 0xc797eb99
firewall#
```

Nell'esempio precedente, l'elenco degli accessi Transit-ACL-Policy ha scartato **19 pacchetti per la porta TCP 2444**, **11 pacchetti per la porta TCP 2556** e **7 pacchetti per la porta TCP 8443** ricevuti da un host o da una rete non attendibile. Inoltre, il messaggio syslog 106023 può fornire preziose informazioni, tra cui l'indirizzo IP di origine e di destinazione, i numeri delle porte di origine e di destinazione e il protocollo IP del pacchetto rifiutato.

Identificazione: Messaggi syslog elenco accessi firewall

Il messaggio syslog del firewall 106023 verrà generato per i pacchetti negati da una voce ACE che non ha la parola chiave **log** presente. 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 regexp* 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 Utilizzo dell'interfaccia della riga di comando.

```
firewall#show logging | grep 106023
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.18/2944 dst
            inside:192.168.1.191/2444 by access-group "Transit-ACL-Policy"
```

```
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.200/2945 dst
            inside:192.168.1.33/2556 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.99/2946 dst
            inside:192.168.1.240/2444 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.2.100/2947 dst
            inside:192.168.1.115/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.4.88/2949 dst
            inside:192.168.1.38/8443 by access-group "Transit-ACL-Policy"
Jun 24 2007 03:25:43: %ASA-4-106023: Deny tcp src outside:192.168.3.175/2950 dst
            inside:192.168.1.250/2444 by access-group "Transit-ACL-Policy"
firewall#
```

Nell'esempio precedente, i messaggi registrati per tACL Transit-ACL-Policy mostrano i pacchetti per la **porta TCP 2444**, i pacchetti per la **porta TCP 2556** e i pacchetti per la **porta TCP 8443** inviati al blocco di indirizzi assegnato all'infrastruttura di rete.

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.

Ulteriori informazioni

Cronologia delle revisioni

Revisione 1.0	11 luglio 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
- Registrazione lista di controllo dell'accesso
- Cisco IOS NetFlow - Home Page su Cisco.com

- White paper su Cisco IOS NetFlow
- Prodotti Cisco Firewall - Home Page su Cisco.com
- Elenco comune delle vulnerabilità e delle esposizioni

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).