

Identificazione e mitigazione dello sfruttamento della vulnerabilità Denial of Service del gateway Cisco Content Services

Identificazione e mitigazione dello sfruttamento della vulnerabilità Denial of Service del gateway Cisco Content Services

ID advisory: cisco-amb-20110706-csg

<https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110706-csg>

Revisione 1.0

Per la Pubblica Release 2011 Luglio 6 16:00 UTC (GMT)

Sommario

[Risposta di Cisco](#)

[Mitigazione e identificazione specifiche del dispositivo](#)

[Ulteriori informazioni](#)

[Cronologia delle revisioni](#)

[Procedure di sicurezza di Cisco](#)

[Informazioni correlate](#)

Risposta di Cisco

Questo bollettino sulla mitigazione applicata è un documento complementare all'advisory della sicurezza PSIRT *Vulnerabilità del rifiuto del servizio del gateway Cisco Content Services* e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

Cisco Content Services Gateway - Second Generation (CSG2) contiene una vulnerabilità quando elabora una serie di pacchetti ICMP realizzati appositamente. Questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo riuscito di questa vulnerabilità può causare il ricaricamento del dispositivo interessato, determinando 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 attraverso una serie di pacchetti ICMP.

A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-2064.

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-20110706-csg>.

Panoramica delle tecniche di mitigazione

I dispositivi Cisco forniscono diverse contromisure per questa 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 essere uno strumento efficace per prevenire gli attacchi tramite gli Access Control List (tACL) di transito.

Questo meccanismo di protezione filtra e scarta i pacchetti che stanno tentando di sfruttare questa vulnerabilità.

Un'efficace prevenzione degli attacchi può essere fornita anche da Cisco ASA serie 5500 Adaptive 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.

Questo meccanismo di protezione filtra e scarta i pacchetti che stanno tentando di sfruttare questa vulnerabilità.

L'uso efficace delle azioni evento di Cisco Intrusion Prevention System (IPS) offre visibilità e protezione dagli attacchi che tentano di sfruttare questa 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 questa 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. La soluzione tACL non è in grado di fornire una protezione completa da questa vulnerabilità quando l'attacco proviene da un indirizzo di origine attendibile.

Il criterio ACL impedisce l'invio ai dispositivi interessati di tipi di pacchetti ICMP non autorizzati, tra cui richiesta echo, risposta echo, host non raggiungibile, traceroute, pacchetto troppo grande, tempo scaduto e non raggiungibile. 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 protocol !
access-list 150 permit icmp host 192.168.100.1
192.168.60.0 0.0.0.255 echo access-list 150 permit icmp host 192.168.100.1
192.168.60.0 0.0.0.255 echo-reply access-list 150 permit icmp host 192.168.100.1
192.168.60.0 0.0.0.255 host-unreachable access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 traceroute access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 packet-too-big access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 time-exceeded access-list 150 permit icmp host
192.168.100.1 192.168.60.0 0.0.0.255 unreachable !!-- The following vulnerability-specific access control entries !-- (ACEs) can aid in identification of attacks !
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 echo access-list 150 deny icmp
any 192.168.60.0 0.0.0.255 echo-reply access-list 150 deny icmp any 192.168.60.0
0.0.0.255 host-unreachable access-list 150 deny icmp any 192.168.60.0 0.0.0.255
traceroute access-list 150 deny icmp any 192.168.60.0 0.0.0.255 packet-too-big
access-list 150 deny icmp any 192.168.60.0 0.0.0.255 time-exceeded access-list 150
deny icmp any 192.168.60.0 0.0.0.255 unreachable !!-- 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 unreachable**. 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 l'ACL a un'interfaccia, il comando **show ip access-lists** restituisce il numero di tipi di pacchetto ICMP filtrati, tra cui richiesta echo, risposta echo, host non raggiungibile, traceroute, pacchetto troppo grande, tempo scaduto e non raggiungibile. Gli amministratori sono invitati a indagare sui pacchetti filtrati per determinare se sono tentativi di sfruttare questa 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 icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo
 20 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo-reply
 30 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 host-unreachable
 40 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 traceroute
 50 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 packet-too-big
 60 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 time-exceeded
 70 permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 unreachable
 80 deny icmp any 192.168.60.0 0.0.0.255 echo (12 matches)
 90 deny icmp any 192.168.60.0 0.0.0.255 echo-reply (26 matches)
100 deny icmp any 192.168.60.0 0.0.0.255 host-unreachable (10 matches)
110 deny icmp any 192.168.60.0 0.0.0.255 traceroute (7 matches)
120 deny icmp any 192.168.60.0 0.0.0.255 packet-too-big (9 matches)
130 deny icmp any 192.168.60.0 0.0.0.255 time-exceeded (2 matches)
140 deny icmp any 192.168.60.0 0.0.0.255 unreachable (18 matches)
150 deny ip any any
router#
```

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

- **12 pacchetti ICMP echo request** per la linea ACE 80
- **26 pacchetti ICMP con risposta echo** per la linea ACE 90
- **10 pacchetti ICMP host-unreachable** per la linea ACE 100
- **7 Pacchetti ICMP traceroute** per la linea ACE 110
- **9 Pacchetti ICMP troppo grandi** per la linea ACE 120
- **2 pacchetti ICMP "time-exceeded"** (tempo scaduto) per ACE line 130
- **18 pacchetti ICMP "destinazione irraggiungibile"** per la linea ACE 140

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.

[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 la vulnerabilità. Si consiglia agli amministratori di analizzare i flussi per determinare se si tratta di tentativi di sfruttare la 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 age 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	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	11393421	2.8	1	48	3.1	0.0	1.4
TCP-FTP	236	0.0	12	66	0.0	1.8	4.8
TCP-FTPD	21	0.0	13726	1294	0.0	18.4	4.1
TCP-WWW	22282	0.0	21	1020	0.1	4.1	7.3
TCP-X	719	0.0	1	40	0.0	0.0	1.3
TCP-BGP	1	0.0	1	40	0.0	0.0	15.0
TCP-Frag	70399	0.0	1	688	0.0	0.0	22.7
TCP-other	47861004	11.8	1	211	18.9	0.0	1.3
UDP-DNS	582	0.0	4	73	0.0	3.4	15.4
UDP-NTP	287252	0.0	1	76	0.0	0.0	15.5
UDP-other	310347	0.0	2	230	0.1	0.6	15.9
ICMP	11674	0.0	3	61	0.0	19.8	15.5
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	4	0.0	1	48	0.0	0.0	15.3
Total:	59957957	14.8	1	196	22.5	0.0	1.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	01	0984	0800	9
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	01	0911	0000	4
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	01	0B3E	0301	5
Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	01	0B89	0030	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	01	0BD7	0200	7
Gi0/0	192.168.15.130	Gi0/1	192.168.60.239	01	0BD7	1100	3
Gi0/0	192.168.23.220	Gi0/1	192.168.60.239	01	0BD7	0300	11
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA	0016	1

```
router#
```

Nell'esempio precedente, sono presenti più flussi per i seguenti tipi di pacchetto **ICMP**: **richiesta echo ICMP (valore esadecimale 0800)**, **echo-reply (valore esadecimale 0000)**, **host-unreachable (valore esadecimale 0301)**, **traceroute (valore esadecimale 0030)**, **packet-to-big (valore esadecimale 0200)**, **time-exceeded (valore esadecimale 1100)**, **time-exceeded (valore esadecimale 0300)**.

Per visualizzare solo i flussi di traffico per i tipi di pacchetto ICMP sopra menzionati, usare il comando **show ip cache flow | include SrcIf|_01_.*(0800|0000|0301|0030|0200|1100|0300)_** visualizzerà i record NetFlow ICMP correlati come mostrato di seguito:

Flussi ICMP

```

router#show ip cache flow | include SrcIf|_01_.*(0800|0000|0301|0030|0200|1100|0300)_
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Gi0/0      192.168.10.201    Gi0/1      192.168.60.102    01 0984 0800   9
Gi0/0      192.168.11.54     Gi0/1      192.168.60.158    01 0911 0000   4
Gi0/0      192.168.13.97     Gi0/1      192.168.60.28     01 0B3E 0301   5
Gi0/0      192.168.10.17     Gi0/1      192.168.60.97     01 0B89 0030   1
Gi0/0      192.168.12.185    Gi0/1      192.168.60.239    01 0BD7 0200   7
Gi0/0      192.168.15.130    Gi0/1      192.168.60.239    01 0BD7 1100   3
Gi0/0      192.168.23.220    Gi0/1      192.168.60.239    01 0BD7 0300  11
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. La soluzione tACL non è in grado di fornire una protezione completa da questa vulnerabilità quando l'attacco proviene da un indirizzo di origine attendibile.

Il criterio ACL impedisce l'invio ai dispositivi interessati di tipi di pacchetti ICMP non autorizzati, tra cui richiesta echo, risposta echo, host non raggiungibile, traceroute, pacchetto troppo grande, tempo scaduto e non raggiungibile. 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 protocol ! access-list tACL-Policy extended permit icmp host
192.168.100.1 192.168.60.0 255.255.255.0 echo access-list tACL-Policy extended permit
icmp host 192.168.100.1 192.168.60.0 255.255.255.0 echo-reply access-list tACL-Policy
extended permit icmp host 192.168.100.1 192.168.60.0 255.255.255.0 traceroute access-
list tACL-Policy extended permit icmp host 192.168.100.1 192.168.60.0 255.255.255.0 2
access-list tACL-Policy extended permit icmp host 192.168.100.1 192.168.60.0
255.255.255.0 time-exceeded access-list tACL-Policy extended permit icmp host
192.168.100.1 192.168.60.0 255.255.255.0 unreachable !!-- The following
vulnerability-specific access control entries !-- (ACEs) can aid in identification of
attacks ! access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
echo access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0 echo-
reply access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
traceroute access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
2 access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0 time-
exceeded access-list tACL-Policy extended deny icmp any 192.168.60.0 255.255.255.0
unreachable !!-- 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
```

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 tipi di pacchetto ICMP filtrati, tra cui richiesta echo, risposta echo, host non raggiungibile, traceroute, pacchetto troppo grande, tempo scaduto e non raggiungibile. Gli amministratori sono invitati a indagare sui pacchetti filtrati per determinare se sono tentativi di sfruttare questa 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; 13 elements
```

```

access-list tACL-Policy line 1 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 echo
access-list tACL-Policy line 2 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 echo-reply
access-list tACL-Policy line 3 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 traceroute
access-list tACL-Policy line 4 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 2
access-list tACL-Policy line 5 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 time-exceeded
access-list tACL-Policy line 6 extended permit icmp host 192.168.100.1
192.168.60.0 255.255.255.0 unreachable
access-list tACL-Policy line 7 extended deny icmp any
192.168.60.0 255.255.255.0 echo (hitcnt=9)
access-list tACL-Policy line 8 extended deny icmp any
192.168.60.0 255.255.255.0 echo-reply (hitcnt=12)
access-list tACL-Policy line 9 extended deny icmp any
192.168.60.0 255.255.255.0 traceroute (hitcnt=7)
access-list tACL-Policy line 10 extended deny icmp any
192.168.60.0 255.255.255.0 2 (hitcnt=11)
access-list tACL-Policy line 11 extended deny icmp any
192.168.60.0 255.255.255.0 time-exceeded (hitcnt=5)
access-list tACL-Policy line 12 extended deny icmp any
192.168.60.0 255.255.255.0 unreachable (hitcnt=8)
access-list tACL-Policy line 13 extended deny ip any any (hitcnt=17)
fireall#

```

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

- **9 pacchetti echo ICMP** per la linea ACE 7
- **12 pacchetti ICMP echo-reply** per la riga ACE 8
- **7 Pacchetti ICMP traceroute** per la linea ACE 9
- **11 pacchetti ICMP troppo grandi** per la linea ACE 10
- **5 pacchetti ICMP "time-exceeded"** (tempo scaduto) per la linea ACE 11
- **8 pacchetti ICMP "destinazione irraggiungibile"** per la linea ACE 12

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 Appliances 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 la vulnerabilità descritta 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
Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.18/2944
dst inside:192.168.60.191/2048 by access-group "tACL-Policy"
Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.2.0.200/2945
dst inside:192.168.60.33/0 by access-group "tACL-Policy"
Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.99/2946
dst inside:192.168.60.240/48 by access-group "tACL-Policy"
Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.100/2947
dst inside:192.168.60.115/512 by access-group "tACL-Policy"
Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.88/2949
dst inside:192.168.60.38/4352 by access-group "tACL-Policy"
Jul 6 2011 00:15:13: %ASA-4-106023: Deny icmp src outside:192.0.2.175/2950
dst inside:192.168.60.250/768 by access-group "tACL-Policy"
```

firewall#

Nell'esempio precedente, i messaggi registrati per il *tACL-Policy* tACL mostrano i tipi di pacchetto **ICMP**, la richiesta **echo**, la risposta **echo**, il **traceroute**, il **pacchetto troppo grande**, il **tempo scaduto** e l'indirizzo **irraggiungibile** inviati 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.

[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 la vulnerabilità descritta in questo documento. A partire dall'aggiornamento della firma S580 per i sensori con Cisco IPS versione 6.x e successive, la vulnerabilità può essere rilevata dalla firma 38247/0 (nome firma: Cisco Content Services Gateway Denial of Service). La firma 38247/0 è abilitata per impostazione predefinita, attiva un evento di gravità *Medio*, ha un indice di fedeltà della firma (SFR) di 90 ed è configurata con un'azione evento predefinita di **produce-alert**.

La firma 38247/0 viene attivata quando vengono rilevati più pacchetti inviati tramite ICMP. L'attivazione di questa firma può indicare un potenziale utilizzo della 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 la vulnerabilità descritta in questo documento.

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

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

[Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco](#)

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

L'appliance Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) può creare incidenti relativi a eventi correlati alla vulnerabilità descritta in questo documento utilizzando la firma IPS 38247/0 (nome della firma: Cisco Content Services Gateway Denial of Service). Dopo aver scaricato l'aggiornamento della firma dinamica S580, utilizzando la parola chiave **NR-38247/0** per la firma IPS 38247/0 e un tipo di query **All Matching Events** on the Cisco Security MARS appliance sarà disponibile un report in cui sono elencati gli incidenti creati dalla firma IPS.

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

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

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

System Rule: CS-MARS IPS Signature Update Failure

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

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

Ulteriori informazioni

IL PRESENTE DOCUMENTO VIENE FORNITO "COSÌ COM'È" E NON IMPLICA ALCUNA GARANZIA O CONCESSIONE, INCLUSE LE GARANZIA DI COMMERCIALIZZABILITÀ 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 1.0	06-luglio-2011	Versione pubblica iniziale
---------------	----------------	----------------------------

Procedure di sicurezza di Cisco

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

Informazioni correlate

- [Bollettini sulla mitigazione applicata da Cisco](#)
- [Cisco Security](#)
- [Servizio Cisco Security IntelliShield Alert Manager](#)
- [Guida Cisco per fortificare i dispositivi Cisco IOS](#)
- [Cisco IOS NetFlow - Home Page su Cisco.com](#)
- [White paper su Cisco IOS NetFlow](#)
- [Analisi delle prestazioni di NetFlow](#)
- [White paper su Cisco Network Foundation Protection](#)
- [Presentazioni di Cisco Network Foundation Protection](#)
- [Un approccio orientato alla sicurezza per l'indirizzamento IP](#)
- [Informazioni sulla protezione del Control Plane](#)
- [Protezione della lingua dei comandi degli strumenti su Cisco IOS](#)
- [Prodotti Cisco Firewall - Home Page su Cisco.com](#)
- [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).