

Identificazione e mitigazione dello sfruttamento della vulnerabilità dello switching dati-link del software Cisco IOS

Identificazione e mitigazione dello sfruttamento della vulnerabilità dello switching dati-link del software Cisco IOS

ID advisory: cisco-amb-20110928-dlsw

<https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110928-dlsw>

Revisione 1.0

Per la Pubblica Release 2011 September 28 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 per la *vulnerabilità dello switching di collegamento dati del software Cisco IOS* e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

Il software Cisco IOS contiene una vulnerabilità durante l'elaborazione di pacchetti DLSw (Data-Link Switching) in formato non corretto. Questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. 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 l'utilizzo è attraverso i pacchetti del protocollo IP 91. Un utente non autorizzato potrebbe sfruttare questa vulnerabilità utilizzando pacchetti di spoofing.

A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0945.

Panoramica delle vulnerabilità

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-20110928-dlsw>.

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 fornire mezzi efficaci di prevenzione degli attacchi utilizzando i seguenti metodi:

- iACL (Access Control List) dell'infrastruttura
- 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 questa vulnerabilità.

L'installazione e la configurazione corrette di RPF unicast offrono un mezzo efficace di protezione dagli attacchi che utilizzano pacchetti con indirizzi IP di origine oggetto di spoofing. È consigliabile distribuire RPF unicast il più vicino possibile a tutte le origini di traffico.

La corretta installazione e configurazione di IPSG fornisce un mezzo efficace di protezione dagli attacchi di spoofing a livello di accesso.

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

- Access Control List (tACL) transit
- RPF unicast

Questi meccanismi di protezione filtrano e rilasciano, oltre a verificare l'indirizzo IP di origine dei pacchetti che stanno tentando 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 Cisco FWSM possono fornire visibilità attraverso i messaggi syslog e i valori dei contatori visualizzati nell'output dei comandi **show**.

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](#)

[Router e switch Cisco IOS](#)

Mitigazione: Access Control List Dell'Infrastruttura

Per proteggere i dispositivi dell'infrastruttura e ridurre al minimo i rischi, l'impatto e l'efficacia degli attacchi diretti all'infrastruttura, gli amministratori devono implementare gli iACL (Access Control List) dell'infrastruttura per applicare le policy relative al traffico inviato ai dispositivi dell'infrastruttura. Gli amministratori possono costruire un iACL autorizzando esplicitamente solo il traffico autorizzato inviato ai dispositivi dell'infrastruttura in base alle configurazioni e ai criteri di sicurezza esistenti. Per garantire la massima protezione dei dispositivi dell'infrastruttura, gli iACL installati devono essere applicati in entrata su tutte le interfacce su cui è stato configurato un indirizzo IP. Una soluzione iACL non può fornire una protezione completa da questa vulnerabilità quando l'attacco proviene da un indirizzo di origine attendibile.

Il criterio iACL nega l'invio ai dispositivi interessati di pacchetti DLSw non autorizzati sul protocollo IP 91. 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. Ove possibile, lo spazio di indirizzi dell'infrastruttura deve essere distinto dallo spazio di indirizzi utilizzato per i segmenti di utenti e servizi. L'uso di questa metodologia di indirizzamento semplificherà la costruzione e l'implementazione degli iACL.

Per ulteriori informazioni sugli iACL, consultare il documento sulla [protezione del core: Access Control List di protezione dell'infrastruttura](#).

```
ip access-list extended Infrastructure-ACL-Policy
!
!-- Include explicit permit statements for trusted sources
!-- that require access on the vulnerable protocol
!
permit 91 host 192.168.100.1 192.168.60.0 0.0.0.255
!
```

```

!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
!
deny 91 any 192.168.60.0 0.0.0.255
!
!-- Explicit deny ACE for traffic sent to addresses configured within
!-- the infrastructure address space
!
deny ip any 192.168.60.0 0.0.0.255
!
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Apply iACL to interfaces in the ingress direction
!
interface GigabitEthernet0/0
ip access-group Infrastructure-ACL-Policy in

```

L'applicazione di un filtro con un elenco degli accessi all'interfaccia determinerà la trasmissione di messaggi ICMP "destinazione irraggiungibile" alla sorgente del traffico filtrato. La generazione di questi messaggi potrebbe avere l'effetto indesiderato di aumentare l'utilizzo della CPU sul dispositivo. Per impostazione predefinita, nel software Cisco IOS la generazione di pacchetti ICMP "destinazione irraggiungibile" è limitata a un pacchetto ogni 500 millisecondi. La generazione di messaggi ICMP "destinazione irraggiungibile" può essere disabilitata usando il comando di configurazione interfaccia **no ip 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**.

Attenuazione: protezione da spoofing

Inoltro percorso inverso unicast

La vulnerabilità descritta in questo documento può essere sfruttata da pacchetti IP oggetto di spoofing. Gli amministratori possono distribuire e configurare Unicast Reverse Path Forwarding (Unicast RPF) come meccanismo di protezione contro lo spoofing.

Unicast RPF è configurato a livello di interfaccia ed è in grado di rilevare ed eliminare pacchetti privi di un indirizzo IP di origine verificabile. Per garantire una protezione completa da spoofing, gli amministratori non devono fare affidamento su RPF unicast, in quanto i pacchetti oggetto di spoofing possono entrare nella rete tramite un'interfaccia abilitata per RPF unicast se esiste una route di ritorno appropriata all'indirizzo IP di origine. È consigliabile che gli amministratori verifichino che durante la distribuzione di questa funzionalità sia configurata la modalità RPF unicast appropriata (libera o rigida), in quanto può causare la perdita di traffico legittimo in transito sulla rete. In un ambiente aziendale, è possibile abilitare RPF unicast sul perimetro Internet e sul livello di accesso interno sulle interfacce di layer 3 supportate dall'utente.

Per ulteriori informazioni, consultare la [guida alla funzionalità di inoltro percorso inverso unicast in modalità alloose](#).

Per ulteriori informazioni sulla configurazione e l'utilizzo di RPF unicast, consultare il [white paper Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence.

Protezione origine IP

IPSG (IP Source Guard) è una funzione di sicurezza che limita il traffico IP su interfacce di layer 2 non indirizzate filtrando i pacchetti in base al database di binding dello snooping DHCP e ai

binding di origine IP configurati manualmente. Gli amministratori possono utilizzare il protocollo IPSG per prevenire gli attacchi degli utenti non autorizzati che tentano di falsificare i pacchetti falsificando l'indirizzo IP di origine e/o l'indirizzo MAC. Se correttamente implementato e configurato, IPSG, insieme a RPF unicast in modalità rigorosa, fornisce i mezzi più efficaci per proteggere da spoofing la vulnerabilità descritta in questo documento.

Per ulteriori informazioni sulla distribuzione e la configurazione di IPSG, consultare il documento sulla [configurazione delle funzionalità DHCP e di IP Source Guard](#).

Identificazione: Access Control List dell'infrastruttura

Dopo che l'amministratore ha applicato l'iACL a un'interfaccia, il comando **show ip access-lists** restituisce il numero di pacchetti DLSw sul protocollo IP 91 che sono stati filtrati sulle interfacce a cui è applicato l'iACL. Gli amministratori devono esaminare i pacchetti filtrati per determinare se sono tentativi di sfruttare questa vulnerabilità. Di seguito è riportato un esempio di output per **show ip access-lists Infrastructure-ACL-Policy**:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
10 permit 91 host 192.168.100.1 192.168.60.0 0.0.0.255
20 deny 91 any 192.168.60.0 0.0.0.255 (8 matches)
30 deny ip any 192.168.60.0 0.0.0.255
router#
```

Nell'esempio precedente, l'elenco degli accessi *Infrastructure-ACL-Policy* ha scartato **8** pacchetti **DLSw** in **Protocollo IP 91** per la riga della voce dell'elenco di controllo degli accessi 20.

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 log/level]** limita l'impatto della generazione e della trasmissione del log.

L'impatto sulla CPU causato dalla registrazione degli ACL può essere risolto tramite hardware sugli switch Cisco Catalyst serie 6500 e sui router Cisco serie 7600 con Supervisor Engine 720 o Supervisor Engine 32 utilizzando la registrazione degli ACL ottimizzata.

Per ulteriori informazioni sulla configurazione e l'utilizzo della registrazione ACL, consultare il [white paper Understanding Access Control List Logging](#) Applied Intelligence.

Identificazione: protezione da spoofing con inoltro percorso inverso unicast

Con RPF unicast implementato e configurato correttamente nell'infrastruttura di rete, gli amministratori possono utilizzare i *comandi* `show cef type slot/port internal`, `show ip interface`, `show cef drop`, `show ip cef switching feature` e `show ip traffic` per identificare il numero di pacchetti scartati da RPF unicast.

Nota: a partire dal software Cisco IOS versione 12.4(20)T, il comando `show ip cef switching` è stato sostituito da `show ip cef switching statistics feature`.

Nota: il *comando* `show | inizio comando regex` e `show | include` i modificatori del comando *regex* vengono utilizzati negli esempi seguenti per ridurre al minimo la quantità di output che gli amministratori dovranno analizzare per visualizzare le informazioni desiderate. Per ulteriori informazioni sui modificatori di comandi, consultare le sezioni [show command](#) della guida di riferimento dei comandi di Cisco IOS Configuration Fundamentals.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
ip verify: via=rx (allow default), acl=0, drop=7, sdrop=0
router#
```

Nota: `show cef interface type slot/port internal` è un comando nascosto che deve essere immesso completamente nell'interfaccia della riga di comando. Il completamento del comando non è disponibile.

```
router#show ip interface GigabitEthernet 0/0 | begin verify
IP verify source reachable-via RX, allow default, allow self-ping 7 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             7           0       0
router#
```

```
router#show ip cef switching statistics feature
```

```
IPv4 CEF input features:
Path Feature Drop    Consume    Punt    Punt2Host  Gave route
RP PAS uRPF          7          0        0        0          0
Total 7 0 0 0 0 -- CLI Output Truncated -- router# router#show ip traffic | include
RPF
```

```
          7 no route,  7 unicast RPF, 0 forced drop
router#
```

Nelle versioni precedenti, `show cef drop`, `show ip cef switching statistics feature`, e `show ip traffic example`, Unicast RPF ha scartato **7 pacchetti IP** ricevuti a livello globale su tutte le interfacce con RPF unicast configurato a causa dell'impossibilità di verificare l'indirizzo di origine dei pacchetti IP nella Forwarding Information Base di Cisco Express Forwarding.

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

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
Gi0/0 192.168.10.201 Gi0/1 192.168.60.102 5B 0000 0000 11
Gi0/0 192.168.11.54 Gi0/1 192.168.60.158 5B 0000 0000 8
Gi0/1      192.168.150.60 Gi0/0      10.89.16.226 06 0016 12CA 1

Gi0/0 192.168.10.17 Gi0/1 192.168.60.97 5B 0000 0000 2
Gi0/0      10.88.226.1 Gi0/1      192.168.202.22 11 007B 007B 1
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 DLSw su Protocollo IP 91 (valore esadecimale 5B).

Questo traffico viene inviato agli indirizzi all'interno del blocco di indirizzi 192.168.60.0/24, che

viene utilizzato dai dispositivi interessati. I pacchetti in questi flussi possono essere oggetto di spoofing e possono indicare un tentativo di sfruttare questa vulnerabilità. Si consiglia agli amministratori di confrontare questi flussi con l'utilizzo di base per il traffico DLSw inviato sul protocollo IP 91 e di esaminare i flussi per determinare se provengono da host o reti non attendibili.

Per visualizzare solo i flussi di traffico per i pacchetti DLSw sul protocollo IP 91 (valore esadecimale 5B), usare il comando **show ip cache flow | include SrcIf_5B_** visualizzerà i record NetFlow del protocollo IP 91 correlati, come mostrato di seguito:

```
router#show ip cache flow | include SrcIf|_5B_
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Gi0/0 192.168.12.110 Gi0/1 192.168.60.163 5B 0000 0000 11
Gi0/0 192.168.11.230 Gi0/1 192.168.60.20 5B 0000 0000 13
Gi0/0 192.168.11.131 Gi0/1 192.168.60.245 5B 0000 0000 7
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 nega i pacchetti DLSw non autorizzati sul protocollo IP 91 inviati ai dispositivi interessati. Nell'esempio seguente, 192.168.60.0/24 è lo spazio di indirizzi IP utilizzato dai dispositivi interessati e l'host con indirizzo 192.168.100.1 è considerato una fonte attendibile che richiede l'accesso ai dispositivi interessati. È necessario prestare attenzione a consentire il traffico richiesto per il routing e l'accesso amministrativo prima di rifiutare tutto il traffico non autorizzato.

Per ulteriori informazioni sugli ACL, consultare il documento [Access Control Lists: Filtering at Your Edge](#) (Liste di controllo dell'accesso in transito: filtraggio sul perimetro della rete).

```
!
!-- Include explicit permit statements for trusted sources
!-- that require access on the vulnerable protocol
! access-list tACL-Policy extended permit 91 host 192.168.100.1 192.168.60.0
255.255.255.0 !
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
! access-list tACL-Policy extended deny 91 any 192.168.60.0 255.255.255.0 !
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Explicit deny for all other IP traffic
! access-list tACL-Policy extended deny ip any any !
!-- Apply tACL to interface(s) in the ingress direction
! access-group tACL-Policy in interface outside
```


Attenuazione: protezione da spoofing con inoltro percorso inverso unicast

La vulnerabilità descritta in questo documento può essere sfruttata da pacchetti IP oggetto di spoofing. Gli amministratori possono distribuire e configurare RPF unicast come meccanismo di protezione contro lo spoofing.

Unicast RPF è configurato a livello di interfaccia ed è in grado di rilevare ed eliminare pacchetti privi di un indirizzo IP di origine verificabile. Per garantire una protezione completa da spoofing, gli amministratori non devono fare affidamento su RPF unicast, in quanto i pacchetti oggetto di spoofing possono entrare nella rete tramite un'interfaccia abilitata per RPF unicast se esiste una route di ritorno appropriata all'indirizzo IP di origine. In un ambiente aziendale, è possibile abilitare RPF unicast sul perimetro Internet e sul livello di accesso interno sulle interfacce di layer 3 supportate dall'utente.

Per ulteriori informazioni sulla configurazione e l'utilizzo di RPF unicast, consultare la guida di riferimento dei comandi di Cisco Security Appliance per [ip verify reverse-path](#) e il white paper [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence.

Identificazione: Access Control List transit

Dopo aver applicato l'ACL a un'interfaccia, gli amministratori possono usare il comando **show access-list** per identificare il numero di pacchetti DLSw sul protocollo IP 91 che sono stati filtrati. 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; 3 elements
access-list tACL-Policy line 1 extended permit 91 host 192.168.100.1
    192.168.60.0 255.255.255.0 (hitcnt=34)
access-list tACL-Policy line 2 extended deny 91 any
    192.168.60.0 255.255.255.0 (hitcnt=6)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

Nell'esempio precedente, l'elenco degli accessi *tACL-Policy* ha scartato **6** pacchetti **DLSw** sul **protocollo IP 91** 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 elenco accessi firewall

Il messaggio syslog del firewall **106023** verrà generato per i pacchetti negati da una voce di controllo di accesso (ACE) che non dispone della parola chiave **log**. Per ulteriori informazioni sul messaggio syslog, consultare il [messaggio Cisco ASA serie 5500 System Log, 8.2 - 106023](#).

Le informazioni sulla configurazione del syslog per Cisco ASA serie 5500 Adaptive Security Appliance sono disponibili in [Monitoraggio - configurazione della registrazione](#). Per informazioni sulla configurazione del syslog sul modulo FWSM per gli switch Cisco Catalyst serie 6500 e i router Cisco serie 7600, consultare il documento sul [monitoraggio del modulo Firewall Services](#).

Nell'esempio seguente, il comando **show logging** | il comando *grep regex* estrae i messaggi syslog dal buffer di registrazione sul firewall. Questi messaggi forniscono informazioni aggiuntive sui pacchetti rifiutati che potrebbero indicare potenziali tentativi di sfruttare 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
```

```
Sep 28 2011 01:10:31: %ASA-4-106023: Deny protocol 91 src outside:192.0.2.18
dst inside:192.168.60.191 by access-group "tACL-Policy"
Sep 28 2011 01:10:31: %ASA-4-106023: Deny protocol 91 src outside:192.0.2.200
dst inside:192.168.60.33 by access-group "tACL-Policy"
Sep 28 2011 01:10:31: %ASA-4-106023: Deny protocol 91 src outside:192.0.2.99
dst inside:192.168.60.240 by access-group "tACL-Policy"
```

```
firewall#
```

Nell'esempio precedente, i messaggi registrati per il *tACL-Policy* mostrano pacchetti **DLSw** potenzialmente oggetto di spoofing per il **protocollo IP 91** 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.

Identificazione: protezione da spoofing con inoltro percorso inverso unicast

Il messaggio syslog del firewall *106021* verrà generato per i pacchetti negati da RPF unicast. Per ulteriori informazioni sul messaggio syslog, consultare il [messaggio Cisco ASA serie 5500 System Log, 8.2 - 106021](#).

Le informazioni sulla configurazione del syslog per Cisco ASA serie 5500 Adaptive Security Appliance sono disponibili in [Monitoraggio - configurazione della registrazione](#). Per informazioni sulla configurazione del syslog sul modulo FWSM per gli switch Cisco Catalyst serie 6500 e i router Cisco serie 7600, consultare il documento sul [monitoraggio del modulo Firewall Services](#).

Nell'esempio seguente, il **comando show logging |** il comando *grep regex* estrae i messaggi syslog dal buffer di registrazione sul firewall. Questi messaggi forniscono informazioni aggiuntive sui pacchetti rifiutati che potrebbero indicare potenziali tentativi di sfruttare 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 106021
```

```
Sep 28 2011 02:00:23: %ASA-1-106021: Deny protocol 91 reverse path check from
192.168.60.1 to 192.168.60.191 on interface outside
Sep 28 2011 02:00:23: %ASA-1-106021: Deny protocol 91 reverse path check from
192.168.60.1 to 192.168.60.33 on interface outside
```

Il comando **show asp drop** può identificare anche il numero di pacchetti scartati dalla funzione

RPF unicast, come mostrato nell'esempio che segue:

```
firewall#show asp drop frame rpf-violated
  Reverse-path verify failed          16
firewall#
```

Nell'esempio precedente, Unicast RPF ha scartato **16 pacchetti** ricevuti su interfacce con Unicast RPF configurato. La mancanza di output indica che la funzionalità RPF unicast sul firewall non ha scartato pacchetti.

Per ulteriori informazioni sul debug di pacchetti o connessioni ignorati dai percorsi di sicurezza accelerati, vedere la guida di riferimento dei comandi di Cisco Security Appliance per [show asp drop](#).

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	2011-SETTEMBRE-28	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](#)
- [Operazioni Cisco Security Intelligence](#)
- [Servizio Cisco Security IntelliShield Alert Manager](#)
- [Guida Cisco per fortificare i dispositivi Cisco IOS](#)
- [Cisco IOS NetFlow - Home Page su Cisco.com](#)
- [White paper su Cisco IOS NetFlow](#)
- [Analisi delle prestazioni di NetFlow](#)
- [White paper su Cisco Network Foundation Protection](#)
- [Presentazioni di Cisco Network Foundation Protection](#)

- [Un approccio orientato alla sicurezza per l'indirizzamento IP](#)
- [Prodotti Cisco Firewall - Home Page su Cisco.com](#)
- [Miglioramenti unicast Reverse Path Forwarding per il provider di servizi Internet](#)
- [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).