Identificazione e mitigazione dello sfruttamento di più vulnerabilità nei prodotti Cisco TelePresence

Identificazione e mitigazione dello sfruttamento di più vulnerabilità nei prodotti Cisco TelePresence

ID advisory: cisco-amb-20110223-telepresence

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110223-telepresence

Revisione 1.1

Per la Pubblica Release 2011 Febbraio 23 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Questo Bollettino sulla mitigazione applicata è un documento complementare al PSIRT Cisco TelePresence Bundle of Security Advisories e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco. I singoli consigli di sicurezza coperti dal presente AMB sono i seguenti:

- Vulnerabilità multiple nei dispositivi endpoint Cisco TelePresence
- Vulnerabilità multiple in Cisco TelePresence Manager
- Vulnerabilità multiple in Cisco TelePresence Multipoint Switch
- Vulnerabilità multiple in Cisco TelePresence Recording Server

Caratteristiche di vulnerabilità

Ci sono diverse vulnerabilità nei prodotti Cisco TelePresence. Le seguenti sottosezioni riepilogano i singoli consigli di sicurezza PSIRT e le rispettive vulnerabilità trattate in ciascun avviso:

Cisco TelePresence Endpoint Devices

Accesso CGI non autenticato: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire l'esecuzione arbitraria del codice. Il vettore di attacco per l'utilizzo è tramite pacchetti HTTP che utilizzano la porta TCP 8082. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0372.

CGI Command Injection: queste vulnerabilità possono essere sfruttate in remoto con l'autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di queste vulnerabilità può consentire l'esecuzione arbitraria del codice. Il vettore di attacco per lo sfruttamento è attraverso pacchetti SSL (Secure Sockets Layer) non validi che utilizzano la porta TCP 443. A queste vulnerabilità sono stati assegnati gli identificatori CVE CVE-2011-0373, CVE-2011-0374 e CVE-2011-0375.

Divulgazione delle informazioni TFTP: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire la divulgazione delle informazioni, che consente all'autore di un attacco di ottenere informazioni sul dispositivo interessato. Il vettore di attacco per lo sfruttamento è tramite i pacchetti di richiesta GET TFTP che utilizzano la porta UDP 69. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0376.

Malicious IP Address Injection: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza interazione dell'utente finale. Se questa vulnerabilità viene sfruttata con successo, è possibile che si verifichi una condizione DoS (Denial of Service) continua. Il vettore di attacco per lo sfruttamento è attraverso pacchetti SOAP (Simple Object Access Protocol) non validi che utilizzano le porte TCP 8081 e 9501. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0377.

Inserimento comando XML-RPC: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire l'esecuzione arbitraria del codice. Il vettore di attacco per l'utilizzo è tramite pacchetti XML-RPC che utilizzano le porte TCP 61441 e 61445. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0378.

Cisco Discovery Protocol Remote Code Execution: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire l'esecuzione arbitraria del codice. Il vettore di attacco per l'utilizzo è tramite i pacchetti del Cisco Discovery Protocol. Poiché il protocollo Cisco Discovery funziona a livello di collegamento dati, l'autore di un attacco deve avere la possibilità di inviare un frame direttamente a un dispositivo interessato. Il presente documento non fornisce ulteriori informazioni per questa vulnerabilità. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0379.

Cisco TelePresence Manager

Bypass autenticazione SOAP: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. Lo sfruttamento di questa vulnerabilità può consentire l'elevazione dei privilegi. Il vettore di attacco per lo sfruttamento è attraverso pacchetti SOAP in formato non corretto che usano le porte TCP 8080 e 8443. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0380.

Iniezione del comando Java Remote Method Invocation (RMI): questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace

di questa vulnerabilità può consentire l'esecuzione arbitraria del codice. Il vettore di attacco per lo sfruttamento è attraverso pacchetti Java RMI creati utilizzando le porte TCP 1100 e 32000. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0381.

Cisco Discovery Protocol Remote Code Execution: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire l'esecuzione arbitraria di codice Il vettore di attacco per l'utilizzo è attraverso i pacchetti del protocollo di rilevamento Cisco. Poiché il protocollo Cisco Discovery funziona a livello di collegamento dati, l'autore di un attacco deve avere la possibilità di inviare un frame direttamente a un dispositivo interessato. Il presente documento non fornisce ulteriori informazioni per questa vulnerabilità. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0379.

Cisco TelePresence Multipoint Switch

Accesso servlet Java non autenticato: queste vulnerabilità possono essere sfruttate in remoto senza autenticazione e senza l'interazione dell'utente finale. Lo sfruttamento efficace di queste vulnerabilità può consentire l'elevazione dei privilegi. Il vettore di attacco per lo sfruttamento è attraverso pacchetti HTTP creati utilizzando le porte TCP 80 e 8080 e pacchetti SSL utilizzando la porta TCP 443. A queste vulnerabilità sono stati assegnati gli identificatori CVE CVE-2011-0383 e CVE-2011-0384.

Caricamento arbitrario di file non autenticato: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire l'esecuzione arbitraria del codice. Il vettore di attacco per lo sfruttamento è attraverso pacchetti HTTP creati utilizzando la porta TCP 80 e pacchetti SSL utilizzando la porta TCP 443. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0385.

Cisco Discovery Protocol Remote Code Execution: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire l'esecuzione arbitraria di codice Il vettore di attacco per l'utilizzo è attraverso i pacchetti del protocollo di rilevamento Cisco. Poiché il protocollo Cisco Discovery funziona a livello di collegamento dati, l'autore di un attacco deve avere la possibilità di inviare un frame direttamente a un dispositivo interessato. Il presente documento non fornisce ulteriori informazioni per questa vulnerabilità. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0379.

Accesso servlet non autorizzato: questa vulnerabilità può essere sfruttata in remoto con l'autenticazione e senza l'interazione dell'utente finale. Lo sfruttamento di questa vulnerabilità può consentire l'elevazione dei privilegi. Il vettore di attacco per l'utilizzo è tramite pacchetti HTTP che utilizzano la porta TCP 80 e pacchetti SSL che utilizzano la porta TCP 443. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0387.

Java RMI Denial of Service: 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 lo sfruttamento è attraverso pacchetti Java RMI creati utilizzando la porta TCP 8999. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0388.

Denial of Service del Real-Time Transport Control Protocol (RTCP): 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 lo sfruttamento è costituito dai pacchetti UDP dannosi inviati a una porta di controllo RTCP in ascolto che viene selezionata casualmente e negoziata durante la configurazione della chiamata. Un utente non autorizzato potrebbe sfruttare questa vulnerabilità utilizzando pacchetti di spoofing. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0389.

Denial of Service XML-RPC: 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 tramite pacchetti XML-RPC che utilizzano la porta TCP 9000. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0390.

Cisco TelePresence Recording Server

Accesso non autenticato al servlet Java: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. Lo sfruttamento di questa vulnerabilità può consentire l'elevazione dei privilegi. Il vettore di attacco per lo sfruttamento è attraverso pacchetti HTTP creati utilizzando le porte TCP 80 e 8080 e pacchetti SSL utilizzando la porta TCP 443. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0383.

Iniezione del comando CGI: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire l'esecuzione arbitraria del codice. Il vettore di attacco per lo sfruttamento è attraverso i pacchetti SSL che utilizzano la porta TCP 443. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0382.

Caricamento arbitrario di file non autenticato: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire l'esecuzione arbitraria del codice. Il vettore di attacco per lo sfruttamento è attraverso pacchetti HTTP creati utilizzando la porta TCP 80 e pacchetti SSL utilizzando la porta TCP 443. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0385.

Sovrascrittura file arbitrari XML-RPC: 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 tramite pacchetti XML-RPC non validi che utilizzano le porte TCP 12102 e 12104. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0386.

Cisco Discovery Protocol Remote Code Execution: questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo efficace di questa vulnerabilità può consentire l'esecuzione arbitraria del codice. Il vettore di attacco per l'utilizzo è tramite i pacchetti del Cisco Discovery Protocol. Poiché il protocollo Cisco Discovery funziona a livello di collegamento dati, l'autore di un attacco deve avere la possibilità di inviare un frame direttamente a un dispositivo interessato. Il presente documento non fornisce ulteriori informazioni per questa vulnerabilità. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0379.

Denial of Service di registrazione ad-hoc: 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 tramite pacchetti HTTP che utilizzano la porta TCP 80. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0391.

Java RMI Denial of Service: 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 lo sfruttamento è attraverso pacchetti Java RMI creati utilizzando la porta TCP 8999. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0388.

Interfaccia XML-RPC non autenticata: questa vulnerabilità può essere sfruttata localmente senza autenticazione e senza l'interazione dell'utente finale. L'efficace sfruttamento di questa vulnerabilità può comportare l'esecuzione di azioni arbitrarie. Il vettore di attacco per l'utilizzo è tramite pacchetti XML-RPC che utilizzano la porta TCP 8080. A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-0392.

Le informazioni sul software vulnerabile, non interessato e fisso sono disponibili nei singoli consigli di sicurezza PSIRT, disponibili ai seguenti link:

- Vulnerabilità multiple nei dispositivi endpoint Cisco TelePresence
- Vulnerabilità multiple in Cisco TelePresence Manager
- Vulnerabilità multiple in Cisco TelePresence Multipoint Switch
- Vulnerabilità multiple in Cisco TelePresence Recording Server

Panoramica delle tecniche di mitigazione

I dispositivi Cisco forniscono diverse contromisure per queste vulnerabilità. Si consiglia agli amministratori di considerare questi metodi di protezione come best practice generali per la sicurezza dei dispositivi dell'infrastruttura e del traffico che attraversa la rete. In questa sezione del documento viene fornita una panoramica di queste tecniche.

Il software Cisco IOS può fornire mezzi efficaci di prevenzione degli attacchi utilizzando i seguenti metodi:

- 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 queste vulnerabilità.

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

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

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

- 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 queste vulnerabilità.

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

I record Cisco IOS NetFlow possono fornire visibilità sui tentativi di sfruttamento basati sulla rete.

I firewall del software Cisco IOS, Cisco ASA e FWSM possono fornire visibilità attraverso i messaggi syslog e i valori dei contatori visualizzati nell'output dei comandi **show**.

L'accessorio Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) può inoltre fornire visibilità attraverso richieste, segnalazioni di incidenti e query.

Per ulteriori informazioni sui vari aspetti da considerare quando si protegge un ambiente Cisco TelePresence, consultare la Cisco TelePresence Hardening Guide.

Gestione dei rischi

Le organizzazioni sono invitate a seguire i processi standard di valutazione e mitigazione dei rischi per determinare l'impatto potenziale di queste vulnerabilità. Triage si riferisce all'ordinamento dei progetti e all'assegnazione delle priorità agli sforzi che hanno maggiori probabilità di avere successo. Cisco ha fornito documenti che possono aiutare le organizzazioni a sviluppare una funzionalità di triage basata sui rischi per i team addetti alla sicurezza delle informazioni. Valutazione dei rischi per la vulnerabilità della sicurezza Gli annunci e la valutazione dei rischi e la creazione di prototipi possono aiutare le organizzazioni a sviluppare processi ripetibili di valutazione della sicurezza e di risposta.

Mitigazione e identificazione specifiche del dispositivo

Attenzione: l'efficacia di qualsiasi tecnica di mitigazione dipende dalle situazioni specifiche del cliente, come il mix di prodotti, la topologia di rete, il comportamento del traffico e la missione organizzativa. Come per qualsiasi modifica apportata alla configurazione, valutare l'impatto della configurazione prima di applicare la modifica.

Per questi dispositivi sono disponibili informazioni specifiche sulla mitigazione e l'identificazione:

- Router e switch Cisco IOS
- Cisco IOS NetFlow
- Cisco ASA e firewall FWSM
- Cisco Intrusion Prevention System
- Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco

Router e switch Cisco IOS

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 queste vulnerabilità quando l'attacco ha origine da un indirizzo di origine attendibile.

Il criterio iACL nega l'autorizzazione dei pacchetti sui protocolli/porte seguenti inviati ai dispositivi interessati:

- porta TCP 80
- porta TCP 443
- porta TCP 1100
- porta TCP 8080
- porta TCP 8081
- porta TCP 8082
- porta TCP 8443
- porta TCP 8999
- porta TCP 9000
- porta TCP 9501
- porta TCP 12102
- porta TCP 12104
- porta TCP 3200
- porta TCP 6141
- porta TCP 6145
- porta UDP 69

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 ports ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 80
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 1100 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 8080 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 8081 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8082 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 8999 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
eq 9000 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9501 permit tcp host
192.168.100.1 192.168.60.0 0.0.0.255 eq 12102 permit tcp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 12104 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255
```

```
eq 32000 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61441 permit tcp
host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61445 permit udp host 192.168.100.1
192.168.60.0 0.0.0.255 eq 69 ! !-- The following vulnerability-specific access
control entries !-- (ACEs) can aid in identification of attacks ! deny tcp any
192.168.60.0 0.0.0.255 eq 80 deny tcp any 192.168.60.0 0.0.0.255 eq 443 deny tcp any
192.168.60.0 0.0.0.255 eq 1100 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 deny tcp
any 192.168.60.0 0.0.0.255 eq 8081 deny tcp any 192.168.60.0 0.0.0.255 eq 8082 deny
tcp any 192.168.60.0 0.0.0.255 eq 8443 deny tcp any 192.168.60.0 0.0.0.255 eq 8999
deny tcp any 192.168.60.0 0.0.0.255 eq 9000 deny tcp any 192.168.60.0 0.0.0.255 eq
9501 deny tcp any 192.168.60.0 0.0.0.255 eq 12102 deny tcp any 192.168.60.0 0.0.0.255
eq 12104 deny tcp any 192.168.60.0 0.0.0.255 eq 32000 deny tcp any 192.168.60.0
0.0.0.255 eq 61441 deny tcp any 192.168.60.0 0.0.0.255 eq 61445 deny udp any
192.168.60.0 0.0.0.255 eq 69 ! !-- 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 unreachables. La limitazione della velocità non raggiungibile ICMP può essere modificata rispetto all'impostazione predefinita utilizzando il comando di configurazione globale ip icmp rate-limit unreachable interval-in-ms.

Attenuazione: protezione da spoofing

Inoltro percorso inverso unicast

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

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

Per ulteriori informazioni, consultare la guida alla funzionalità di inoltro percorso inverso unicast in modalità alloose.

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

Protezione origine IP

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

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

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

Identificazione: Access Control List dell'infrastruttura

Dopo che l'amministratore ha applicato l'iACL a un'interfaccia, il comando show ip access-lists identificherà i pacchetti sui seguenti protocolli/porte che sono stati filtrati sulle interfacce a cui l'iACL è applicato:

- porta TCP 80
- porta TCP 443
- porta TCP 1100
- porta TCP 8080
- porta TCP 8081
- porta TCP 8082
- porta TCP 8443
- porta TCP 8999
- porta TCP 9000
- porta TCP 9501
- porta TCP 12102
- porta TCP 12104
- porta TCP 3200
- porta TCP 6141
- porta TCP 6145
- porta UDP 69

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 gli elenchi degli accessi show ip:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq www
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    30 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 1100
    40 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8080
    50 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8081
    60 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8082
    70 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 (1 match)
    80 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8999
    90 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9000
    100 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 9501
    110 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 12102
    120 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 12104
    130 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 32000
    140 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61441
    150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 61445
```

```
    160 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq tftp
    170 deny tcp any 192.168.60.0 0.0.0.255 eq www (703 matches)
    180 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (213 matches)
    190 deny tcp any 192.168.60.0 0.0.0.255 eq 1100 (95 matches)
    200 deny tcp any 192.168.60.0 0.0.0.255 eq 8080 (115 matches)
    210 deny tcp any 192.168.60.0 0.0.0.255 eq 8081 (119 matches)
    220 deny tcp any 192.168.60.0 0.0.0.255 eq 8082 (86 matches)
    230 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (125 matches)
    240 deny tcp any 192.168.60.0 0.0.0.255 eq 8999 (63 matches)
    250 deny tcp any 192.168.60.0 0.0.0.255 eq 9000 (3 matches)
    260 deny tcp any 192.168.60.0 0.0.0.255 eq 9501 (142 matches)
    270 deny tcp any 192.168.60.0 0.0.0.255 eq 12102 (127 matches)
    280 deny tcp any 192.168.60.0 0.0.0.255 eq 12104 (132 matches)
    290 deny tcp any 192.168.60.0 0.0.0.255 eq 32000 (125 matches)
    300 deny tcp any 192.168.60.0 0.0.0.255 eq 61441 (110 matches)
    310 deny tcp any 192.168.60.0 0.0.0.255 eq 61445 (114 matches)
    320 deny udp any 192.168.60.0 0.0.0.255 eq tftp (218 matches)
    330 deny ip any 192.168.60.0 0.0.0.255 (9 matches)
router#
```

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

- 703 pacchetti HTTP sulla porta TCP 80 (www) per la linea ACE 170
- 213 pacchetti SSL sulla porta TCP 443 per la linea ACE 180
- 95 pacchetti sulla porta TCP 1100 per la linea ACE 190
- 115 pacchetti sulla porta TCP 8080 per la linea ACE 200
- 119 pacchetti sulla porta TCP 8081 per la linea ACE 210
- 86 pacchetti sulla porta TCP 8082 per la linea ACE 220
- 125 pacchetti sulla porta TCP 8443 per la linea ACE 230
- 63 pacchetti sulla porta TCP 8999 per la linea ACE 240
- 3 pacchetti sulla porta TCP 9000 per la linea ACE 250
- 142 pacchetti sulla porta TCP 9501 per la linea ACE 260
- 127 pacchetti sulla porta TCP 12102 per la linea ACE 270
- 132 pacchetti sulla porta TCP 12104 per la linea ACE 280
- 125 pacchetti sulla porta TCP 3200 per la linea ACE 290
- 110 pacchetti sulla porta TCP 61441 per la linea ACE 300
- 114 pacchetti sulla porta TCP 61445 per la linea ACE 310
- 218 pacchetti TFTP sulla porta UDP 69 per la linea ACE 320

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 di 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 di 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 sono utilizzati negli esempi seguenti per ridurre al minimo la quantità di output che gli amministratori dovranno analizzare per visualizzare le informazioni desiderate. Per ulteriori informazioni sui modificatori di comandi, consultare le sezioni show command della guida di riferimento dei comandi di Cisco IOS Configuration Fundamentals.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop

ip verify: via=rx (allow default), acl=0, drop=18, sdrop=0
router#
```

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

```
router#show ip interface GigabitEthernet 0/0 | begin verify

        IP verify source reachable-via RX, allow default, allow self-ping
        18 verification drops
        0 suppressed verification drops
router#
```

```
router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported    No_route      No_adj  ChkSum_Err
RP            27           0           0          18           0           0
router#
```

```
router#show ip cef switching statistics feature
IPv4 CEF input features:
Path   Feature                Drop    Consume       Punt  Punt2Host Gave route
RP PAS uRPF                     18          0          0          0          0
Total                           18          0          0          0          0
--      CLI Output Truncated       --
router#

router#show ip traffic | include RPF
           18 no route, 18 unicast RPF, 0 forced drop
router#
```

Nelle versioni precedenti, **show cef drop**, **show ip cef switching statistics feature** e **show ip traffic** example, Unicast RPF ha scartato **18 pacchetti IP** ricevuti a livello globale su tutte le interfacce con RPF unicast configurato a causa dell'impossibilità di verificare l'indirizzo di origine dei pacchetti IP nella base di informazioni sull'inoltro di Cisco Express Forwarding.

Cisco IOS NetFlow

Identificazione: Identificazione del flusso di traffico mediante i record NetFlow

Gli amministratori possono configurare Cisco IOS NetFlow sui router e gli switch Cisco IOS per aiutare a identificare i flussi di traffico che potrebbero essere tentativi di sfruttare queste vulnerabilità. Si consiglia agli amministratori di analizzare i flussi per determinare se si tratta di tentativi di sfruttare queste vulnerabilità o se si tratta di flussi di traffico legittimi.

```
router#show ip cache flow

IP packet size distribution (1779 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .323 .676 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

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

IP Flow Switching Cache, 278544 bytes
  183 active, 3913 inactive, 364 added
  4883 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 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-WWW             16      0.0         7    40      0.0       0.0      15.7
TCP-other          126      0.0         3    40      0.1       0.0      15.4
UDP-TFTP             7      0.0         6    28      0.0       0.0      15.6
UDP-other           32      0.0         6    28      0.0       0.0      15.4
Total:             181      0.0         4    36      0.1       0.0      15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.21.36   Et0/1         192.168.60.17   11 CD3E 0045     1
Et0/0         192.168.100.31  Et0/1         192.168.60.210  06 8F8C 044C     6
Et0/0         192.168.100.14  Et0/1         192.168.60.121  06 DEBB 251D     3
Et0/0         192.168.100.209 Et0/1         192.168.60.19   06 C460 1F90     3
```

```
Et0/0         192.168.100.235 Et0/1         192.168.60.15   06 46E6 7D00     1
Et0/0         192.168.159.166 Et0/1         192.168.90.53   11 62E2 B413    10
Et0/0         192.168.100.164 Et0/1         192.168.60.91   06 5460 2F46     3
Et0/0         192.168.100.83  Et0/1         192.168.60.30   06 E440 1F92     6
Et0/0         192.168.12.204  Et0/1         192.168.162.10  11 39D3 9273    10
Et0/0         192.168.100.211 Et0/1         192.168.60.174  06 846A 1F91     4
Et0/0         192.168.100.112 Et0/1         192.168.60.242  06 4F39 044C     3
Et0/0         192.168.100.147 Et0/1         192.168.60.153  06 9B55 0050    15
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2327     4
Et0/0         192.168.100.188 Et0/1         192.168.60.26   06 E9AC 2328     4
Et0/0         192.168.194.210 Et0/1         192.168.4.64    11 85DE BE0C     5
Et0/0         192.168.100.171 Et0/1         192.168.60.215  06 84F3 1F91     1
Et0/0         192.168.100.121 Et0/1         192.168.60.165  06 15A0 2F48     8
Et0/0         192.168.100.97  Et0/1         192.168.60.22   06 0951 2327     1
Et0/0         192.168.100.221 Et0/1         192.168.60.170  06 DBCF 0050    10
Et0/0         192.168.6.90    Et0/1         192.168.243.120 06 14E7 773D    10
Et0/0         192.168.100.174 Et0/1         192.168.60.239  06 0414 1F91     5
Et0/0         192.168.100.51  Et0/1         192.168.60.109  06 EF9D 251D     2
Et0/0         192.168.78.53   Et0/1         192.168.60.37   11 07A2 0045     2
Et0/0         192.168.164.19  Et0/1         192.168.201.180 06 FA1C 557B     5
Et0/0         192.168.66.15   Et0/1         192.168.155.182 11 FBC6 585A     3
Et0/0         192.168.100.208 Et0/1         192.168.60.137  06 BEC3 20FB     1
Et0/0         192.168.100.43  Et0/1         192.168.60.70   06 5E31 01BB    14
Et0/0         192.168.100.43  Et0/1         192.168.60.0    06 0FAA F001     1
Et0/0         192.168.29.205  Et0/1         192.168.240.249 11 71B3 8F9C     8
Et0/0         192.168.100.179 Et0/1         192.168.60.214  06 A2C4 F005     4
Et0/0         192.168.89.13   Et0/1         192.168.204.26  11 1D17 2CB0    11
router#
```

Nell'esempio precedente sono presenti più flussi per:

- HTTP sulla porta TCP 80 (valore esadecimale 0050)
- SSL sulla porta TCP 443 (valore esadecimale 01BB)
- Porta TCP 1100 (valore esadecimale 044C)
- Porta TCP 8080 (valore esadecimale 1F90)
- Porta TCP 8081 (valore esadecimale 1F91)
- Porta TCP 8082 (valore esadecimale 1F92)
- Porta TCP 8443 (valore esadecimale 20FB)
- Porta TCP 8999 (valore esadecimale 2327)
- Porta TCP 9000 (valore esadecimale 2328)
- Porta TCP 9501 (valore esadecimale 251D)
- Porta TCP 12102 (valore esadecimale 2F46)
- Porta TCP 12104 (valore esadecimale 2F48)
- Porta TCP 3200 (valore esadecimale 7D00)
- Porta TCP 61441 (valore esadecimale F001)
- Porta TCP 61445 (valore esadecimale F005)
- TFTP sulla porta UDP 69 (valore esadecimale 0045)

Il traffico ha origine e viene inviato agli indirizzi inclusi nel blocco di indirizzi 192.168.60.0/24, utilizzato per i dispositivi dell'infrastruttura. I pacchetti in questi flussi possono essere oggetto di spoofing e possono indicare un tentativo di sfruttare queste vulnerabilità. Si consiglia agli amministratori di confrontare questi flussi con l'utilizzo di base per il traffico inviato sui protocolli/porte indicati 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 sulle porte/protocolli indicati, usare il comando show ip cache flow | include SrcIf|__11_.*0045 visualizzerà i record NetFlow UDP correlati, come mostrato di seguito:

Flussi UDP

```
router#show ip cache flow | include SrcIf|_11_.*0045
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

Et0/0         192.168.54.222  Et0/1         192.168.60.43   11 7947 0045     3
Et0/0         192.168.247.117 Et0/1         192.168.60.169  11 45FB 0045     1
Et0/0         192.168.250.16  Et0/1         192.168.60.79   11 66AC 0045    10
Et0/0         192.168.121.112 Et0/1         192.168.60.36   11 6725 0045    16
Et0/0         192.168.243.192 Et0/1         192.168.60.225  11 2B52 0045     1
router#
```

Per visualizzare solo i flussi di traffico per i pacchetti sulle porte/protocolli indicati, usare il comando show ip cache flow | include SrcIf|__06_.*(0050|01BB|044C|1F90|1F91|1F92|20FB|2327|2328|251D|2F46|2F48|7D00|F001|F005)_ visualizza i record TCP NetFlow correlati come mostrato di seguito:

Flussi TCP

```
router#show ip cache flow | include
SrcIf|_06_.*(0050|01BB|044C|1F90|1F91|1F92|20FB|2327|2328|251D|2F46|2F48|7D00|F001|F0
05)_
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.100.14  Et0/1          192.168.60.121  06 DEBB 251D     3
Et0/0         192.168.100.209 Et0/1          192.168.60.19   06 C460 1F90     3
Et0/0         192.168.100.235 Et0/1          192.168.60.15   06 46E6 7D00     1
Et0/0         192.168.100.164 Et0/1          192.168.60.91   06 5460 2F46     3
Et0/0         192.168.100.83  Et0/1          192.168.60.30   06 E440 1F92     6

Et0/0         192.168.100.211 Et0/1          192.168.60.174  06 846A 1F91     4
Et0/0         192.168.100.112 Et0/1          192.168.60.242  06 4F39 044C     3
Et0/0         192.168.100.147 Et0/1          192.168.60.153  06 9B55 0050    15
Et0/0         192.168.100.188 Et0/1          192.168.60.26   06 E9AC 2327     4
Et0/0         192.168.100.188 Et0/1          192.168.60.26   06 E9AC 2328     4

Et0/0         192.168.100.121 Et0/1          192.168.60.165  06 15A0 2F48     8

Et0/0         192.168.100.208 Et0/1          192.168.60.137  06 BEC3 20FB     1
Et0/0         192.168.100.43  Et0/1          192.168.60.70   06 5E31 01BB    14
Et0/0         192.168.100.43  Et0/1          192.168.60.0    06 0FAA F001     1
Et0/0         192.168.100.179 Et0/1          192.168.60.214  06 A2C4 F005     4

Et0/0         192.168.100.209 Et0/1          192.168.60.19   06 C460 1F90     3
router#
```

Cisco ASA e firewall FWSM

Attenuazione: Access Control List transit

Per proteggere la rete dal traffico che entra nei punti di accesso in entrata, che possono includere punti di connessione Internet, punti di connessione fornitori e partner o punti di connessione VPN, si consiglia agli amministratori di distribuire gli ACL per applicare la policy. Gli amministratori possono costruire un ACL autorizzando esplicitamente solo il traffico autorizzato ad accedere alla rete dai punti di accesso in entrata o autorizzando il traffico autorizzato a transitare sulla rete in base alle configurazioni e ai criteri di sicurezza esistenti. Una soluzione ACL non può fornire una protezione completa da queste vulnerabilità quando l'attacco ha origine da un indirizzo di origine

attendibile.

Il criterio ACL nega l'autorizzazione dei pacchetti non autorizzati sui protocolli/porte seguenti inviati ai dispositivi interessati:

- porta TCP 80
- porta TCP 443
- porta TCP 1100
- porta TCP 8080
- porta TCP 8081
- porta TCP 8082
- porta TCP 8443
- porta TCP 8999
- porta TCP 9000
- porta TCP 9501
- porta TCP 12102
- porta TCP 12104
- porta TCP 3200
- porta TCP 6141
- porta TCP 6145
- porta UDP 69

Nell'esempio seguente, 192.168.60.0/24 è lo spazio di indirizzi IP utilizzato dai dispositivi interessati e l'host con indirizzo 192.168.100.1 è considerato una fonte attendibile che richiede l'accesso ai dispositivi interessati. È necessario prestare attenzione a consentire il traffico richiesto per il routing e l'accesso amministrativo prima di rifiutare tutto il traffico non autorizzato.

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

```
! !-- Include explicit permit statements for trusted sources !-- that require access
on the vulnerable ports ! access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 80 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 443 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 1100
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 8080 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8081 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 8082 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8443 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 8999
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 9000 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9501 access-list tACL-Policy extended permit tcp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 12102 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 12104 access-list tACL-
Policy extended permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 32000
access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 61441 access-list tACL-Policy extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61445 access-list tACL-Policy extended permit udp host
192.168.100.1 192.168.60.0 255.255.255.0 eq 69 ! !-- The following vulnerability-
specific access control entries !-- (ACEs) can aid in identification of attacks !
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 80
```

```
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 1100
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8080
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8081
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8082
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8999
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 9000
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 9501
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 12102
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 12104
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 32000
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 61441
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 61445
access-list tACL-Policy extended deny udp any 192.168.60.0 255.255.255.0 eq 69 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-- with existing security policies and configurations ! !-- Explicit deny for all other IP traffic !
access-list tACL-Policy extended deny ip any any ! !-- Apply tACL to interface(s) in the ingress direction ! access-group tACL-Policy in interface outside
```

Attenuazione: protezione da spoofing con inoltro percorso inverso unicast

Le vulnerabilità descritte in questo documento possono essere sfruttate da pacchetti IP oggetto di spoofing. Gli amministratori possono distribuire e configurare RPF unicast come meccanismo di protezione contro lo spoofing.

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

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

Identificazione: Access Control List transit

Dopo aver applicato l'ACL a un'interfaccia, gli amministratori possono utilizzare il comando show access-list per identificare i protocolli/porte seguenti a cui è stato applicato un filtro:

- porta TCP 80
- porta TCP 443
- porta TCP 1100
- porta TCP 8080
- porta TCP 8081
- porta TCP 8082
- porta TCP 8443
- porta TCP 8999
- porta TCP 9000
- porta TCP 9501
- porta TCP 12102

- porta TCP 12104
- porta TCP 3200
- porta TCP 6141
- porta TCP 6145
- porta UDP 69

Gli amministratori sono invitati a indagare sui pacchetti filtrati per determinare se sono tentativi di sfruttare queste vulnerabilità. Di seguito è riportato un esempio di output per show access-list tACL-Policy:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 31 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq www (hitcnt=55)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq https (hitcnt=765)
access-list tACL-Policy line 3 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 1100 (hitcnt=43)
access-list tACL-Policy line 4 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8080 (hitcnt=265)
access-list tACL-Policy line 5 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8081 (hitcnt=18)
access-list tACL-Policy line 6 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8082 (hitcnt=77)
access-list tACL-Policy line 7 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8443 (hitcnt=345)
access-list tACL-Policy line 8 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 8999 (hitcnt=137)
access-list tACL-Policy line 9 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9000 (hitcnt=17)
access-list tACL-Policy line 10 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 9501 (hitcnt=36)
access-list tACL-Policy line 11 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 12102 (hitcnt=40)
access-list tACL-Policy line 12 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 12104 (hitcnt=23)
access-list tACL-Policy line 13 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 32000 (hitcnt=109)
access-list tACL-Policy line 14 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61441 (hitcnt=60)
access-list tACL-Policy line 15 extended permit tcp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 61445 (hitcnt=95)
access-list tACL-Policy line 16 extended permit udp host 192.168.100.1
192.168.60.0 255.255.255.0 eq tftp (hitcnt=4567)
access-list tACL-Policy line 17 extended deny tcp any
192.168.60.0 255.255.255.0 eq www (hitcnt=28)
access-list tACL-Policy line 18 extended deny tcp any
192.168.60.0 255.255.255.0 eq https (hitcnt=169)
access-list tACL-Policy line 19 extended deny tcp any
192.168.60.0 255.255.255.0 eq 1100 (hitcnt=93)
access-list tACL-Policy line 20 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8080 (hitcnt=11)
access-list tACL-Policy line 21 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8081 (hitcnt=9)
access-list tACL-Policy line 22 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8082 (hitcnt=9)
access-list tACL-Policy line 23 extended deny tcp any
192.168.60.0 255.255.255.0 eq 8443 (hitcnt=34)
access-list tACL-Policy line 24 extended deny tcp any
```

```
192.168.60.0 255.255.255.0 eq 8999 (hitcnt=46)
access-list tACL-Policy line 25 extended deny tcp any
192.168.60.0 255.255.255.0 eq 9000 (hitcnt=6)
access-list tACL-Policy line 26 extended deny tcp any
192.168.60.0 255.255.255.0 eq 9501 (hitcnt=9)
access-list tACL-Policy line 27 extended deny tcp any
192.168.60.0 255.255.255.0 eq 12102 (hitcnt=11)
access-list tACL-Policy line 28 extended deny tcp any
192.168.60.0 255.255.255.0 eq 12104 (hitcnt=24)
access-list tACL-Policy line 29 extended deny tcp any
192.168.60.0 255.255.255.0 eq 32000 (hitcnt=48)
access-list tACL-Policy line 30 extended deny tcp any
192.168.60.0 255.255.255.0 eq 61441 (hitcnt=32)
access-list tACL-Policy line 31 extended deny tcp any
192.168.60.0 255.255.255.0 eq 61445 (hitcnt=9)
access-list tACL-Policy line 32 extended deny udp any
192.168.60.0 255.255.255.0 eq tftp (hitcnt=78)
access-list tACL-Policy line 33 extended deny ip any any (hitcnt=4658)
firewall#
```

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

- 28 pacchetti HTTP sulla porta TCP 80 (www) per la riga ACE 17
- 169 pacchetti SSL sulla porta TCP 443 (https) per la linea ACE 18
- 93 pacchetti sulla porta TCP 1100 per la linea ACE 19
- 11 pacchetti sulla porta TCP 8080 per la linea ACE 20
- 9 pacchetti sulla porta TCP 8081 per la linea ACE 21
- 9 pacchetti sulla porta TCP 8082 per la linea ACE 22
- 34 pacchetti sulla porta TCP 8443 per la linea ACE 23
- 46 pacchetti sulla porta TCP 8999 per la linea ACE 24
- 6 pacchetti sulla porta TCP 9000 per la linea ACE 25
- 9 pacchetti sulla porta TCP 9501 per la linea ACE 26
- 11 pacchetti sulla porta TCP 12102 per la linea ACE 27
- 24 pacchetti sulla porta TCP 12014 per la linea ACE 28
- 48 pacchetti sulla porta TCP 3200 per la linea ACE 29
- 32 pacchetti sulla porta TCP 61441 per la linea ACE 30
- 9 pacchetti sulla porta TCP 61445 per la linea ACE 31
- 78 pacchetti TFTP sulla porta UDP 69 (tftp) per la linea ACE 32

Identificazione: Messaggi syslog elenco accessi firewall

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

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

Nell'esempio seguente, il comando show logging | il comando grep regex estrae i messaggi syslog dal buffer di registrazione sul firewall. Questi messaggi forniscono informazioni aggiuntive sui pacchetti rifiutati che potrebbero indicare potenziali tentativi di sfruttare le vulnerabilità descritte in questo documento. È possibile utilizzare espressioni regolari diverse 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
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.215/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.173/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:41: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/80 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:48: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/443 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.225.47/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:57:55: %ASA-4-106023: Deny tcp src outside:192.168.156.169/1024
                  dst inside:192.168.60.25/1100 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.191.223/1024
                  dst inside:192.168.60.103/8080 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.25/8080 by access-group "tACL-Policy"
  Jan 12 2011 14:58:02: %ASA-4-106023: Deny tcp src outside:192.168.1.1/1024
                  dst inside:192.168.60.177/8080 by access-group "tACL-Policy"
firewall#
```

Nell'esempio precedente, i messaggi registrati per i criteri tACL tACL mostrano i pacchetti HTTP per la porta TCP 80, i pacchetti SSL per la porta TCP 443, i pacchetti per la porta TCP 1100 e i pacchetti per la porta TCP 8080 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

Verrà generato il messaggio syslog del firewall 106021 per i pacchetti negati da RPF unicast. Per ulteriori informazioni sul messaggio syslog, consultare il messaggio Cisco ASA serie 5500 System Log, 8.2 - 106021.

Le informazioni sulla configurazione del syslog per Cisco ASA serie 5500 Adaptive Security Appliance sono disponibili in Monitoraggio - configurazione della registrazione. Per informazioni sulla configurazione del syslog sul modulo FWSM per gli switch Cisco Catalyst serie 6500 e i

router Cisco serie 7600, consultare il documento sul monitoraggio del modulo Firewall Services.

Nell'esempio seguente, il **comando show logging | il** comando **grep** regex estrae i messaggi syslog dal buffer di registrazione sul firewall. Questi messaggi forniscono informazioni aggiuntive sui pacchetti rifiutati che potrebbero indicare potenziali tentativi di sfruttare le vulnerabilità descritte in questo documento. È possibile utilizzare diverse espressioni regolari con la parola chiave **grep** per cercare dati specifici nei messaggi registrati.

Per ulteriori informazioni sulla sintassi delle espressioni regolari, vedere Creazione di un'espressione regolare.

```
firewall#show logging | grep 106021
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny UDP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
        Feb 21 2010 00:15:13: %ASA-1-106021: Deny TCP reverse path check from

                    192.168.60.1 to 192.168.60.100 on interface outside
```

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

```
firewall#show asp drop frame rpf-violated
        Reverse-path verify failed                      11
firewall#
```

Nell'esempio precedente, Unicast RPF ha scartato **11 pacchetti IP** ricevuti su interfacce con Unicast RPF configurato. La mancanza di output indica che la funzionalità RPF unicast sul firewall non ha scartato pacchetti.

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

Cisco Intrusion Prevention System

Attenuazione: azioni evento firma Cisco IPS

Gli amministratori possono utilizzare gli accessori e i moduli dei servizi di Cisco Intrusion Prevention System (IPS) per rilevare le minacce e prevenire i tentativi di sfruttare le vulnerabilità descritte nel presente documento. Queste vulnerabilità possono essere rilevate dalle seguenti firme:

- 32719-0: Esecuzione Comandi Arbitrari Remoti Non Autenticati Di Cisco Telepresence
- 3859-0: Cisco TelePresence Endpoint CGI Command Injection
- 3860-0: Cisco TelePresence Multipoint Switch Java Servlet Access
- 3860-1: Cisco TelePresence Multipoint Switch Java Servlet Access
- 3861-0: Vulnerabilità dell'esecuzione dei comandi del server di registrazione Cisco TelePresence

32719-0: Esecuzione Comandi Arbitrari Remoti Non Autenticati Di Cisco Telepresence

A partire dall'aggiornamento della firma S550 per i sensori che eseguono Cisco IPS versione 6.x e successive, queste vulnerabilità possono essere rilevate dalla firma 32719/0 (nome della firma: Cisco Telepresence Unauthenticated Remote Arbitrary Command Execution). La firma 32719/0 è abilitata per impostazione predefinita, attiva un evento di alta gravità, ha un indice di fedeltà della firma (SFR) di 90 ed è configurata con un'azione evento predefinita di **produce-alert**.

La firma 32719/0 viene attivata su un tentativo di sfruttare una vulnerabilità nell'esecuzione di un comando arbitrario remoto non autenticato in un endpoint Cisco TelePresence inviato tramite la porta TCP 8082. L'attivazione di questa firma può indicare un potenziale sfruttamento di queste vulnerabilità.

3859-0: Cisco TelePresence Endpoint CGI Command Injection

A partire dall'aggiornamento della firma S550 per i sensori con Cisco IPS versione 6.x e successive, queste vulnerabilità possono essere rilevate dalla firma 33859-0 (nome firma: Cisco TelePresence Endpoint CGI Command Injection). La firma 3859/0 è abilitata per impostazione predefinita, attiva un evento di alta gravità, ha un indice di fedeltà della firma (SFR) di 80 ed è configurata con un'azione evento predefinita di **produce-alert**.

La firma 3859/0 viene attivata su un tentativo di sfruttare una vulnerabilità nell'esecuzione di un comando arbitrario remoto non autenticato in un endpoint Cisco TelePresence inviato tramite la porta TCP 8082. L'attivazione di questa firma può indicare un potenziale sfruttamento di queste vulnerabilità.

3860-0: Cisco TelePresence Multipoint Switch Java Servlet Access

A partire dall'aggiornamento della firma S550 per i sensori che eseguono Cisco IPS versione 6.x e successive, queste vulnerabilità possono essere rilevate dalla firma 33860-0 (nome firma: Cisco TelePresence Multipoint Switch Java Servlet Access). La firma 3860/0 è disabilitata per impostazione predefinita, attiva un evento di alta gravità, ha un indice di fedeltà della firma (SFR) di 75 ed è configurata con un'azione evento predefinita di **produce-alert**.

La firma 3860/0 viene attivata al rilevamento dell'accesso di diversi servlet Java all'interno di Cisco TelePresence Multipoint Switch inviato tramite la porta TCP 8080. L'attivazione di questa firma può indicare un potenziale sfruttamento di queste vulnerabilità.

Nota: questa firma può essere attivata in modo non dannoso sui dispositivi che non sono Cisco TelePresence Multipoint Switch. Sono necessarie ulteriori indagini per eliminare tali dispositivi.

3860-1: Cisco TelePresence Multipoint Switch Java Servlet Access

A partire dall'aggiornamento della firma S550 per i sensori che eseguono Cisco IPS versione 6.x e successive, queste vulnerabilità possono essere rilevate dalla firma 33860-1 (nome firma: Cisco TelePresence Multipoint Switch Java Servlet Access). La firma 3860/1 è disabilitata per impostazione predefinita, attiva un evento di alta gravità, ha un indice di fedeltà della firma (SFR) di 75 ed è configurata con un'azione evento predefinita di **produzione-avviso**.

La firma 3860/1 viene attivata al rilevamento dell'accesso di diversi servlet Java all'interno di Cisco TelePresence Multipoint Switch inviato tramite la porta TCP 80. L'attivazione di questa firma può indicare un potenziale sfruttamento di queste vulnerabilità.

Nota: questa firma può essere attivata in modo non dannoso sui dispositivi che non sono Cisco

TelePresence Multipoint Switch. Sono necessarie ulteriori indagini per eliminare tali dispositivi.

3861-0: Vulnerabilità dell'esecuzione dei comandi del server di registrazione Cisco TelePresence

A partire dall'aggiornamento della firma S550 per i sensori con Cisco IPS versione 6.x e successive, queste vulnerabilità possono essere rilevate dalla firma 33861/0 (nome firma: Cisco TelePresence Recording Server Command Execution Vulnerability). La firma 3861/0 è abilitata per impostazione predefinita, attiva un evento di alta gravità, ha un indice di fedeltà della firma (SFR) di 90 ed è configurata con un'azione evento predefinita di **produce-alert**.

Questa firma viene generata quando viene rilevato un tentativo di sfruttare una vulnerabilità specifica dell'esecuzione dei comandi in Cisco TelePresence Recording Server. Questa vulnerabilità è ulteriormente documentata in CVE-2011-0382.

La firma 33861/0 è una meta-firma ed è composta da più sottofirme (Signature ID da 33861-1 a 33861-4) che devono essere attivate per attivare la meta-firma. Ciascuna delle singole sottoscrizioni pertanto non dispone di un'azione evento e pertanto ciascuna di esse viene considerata un evento di gravità Informativo.

Gli amministratori possono configurare i sensori Cisco IPS in modo da eseguire un'azione evento quando viene rilevato un attacco. L'azione evento configurata esegue controlli preventivi o deterrenti per contribuire alla protezione da un attacco che tenta di sfruttare le vulnerabilità descritte in questo documento.

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

- 32719-0: Esecuzione Comandi Arbitrari Remoti Non Autenticati Di Cisco Telepresence
- 3859-0: Cisco TelePresence Endpoint CGI Command Injection
- 3860-0: Cisco TelePresence Multipoint Switch Java Servlet Access
- 3860-1: Cisco TelePresence Multipoint Switch Java Servlet Access
- 3861-0: Vulnerabilità dell'esecuzione dei comandi del server di registrazione Cisco TelePresence

Dopo aver scaricato l'aggiornamento della firma dinamica S550, utilizzando le parole chiave seguenti per i rispettivi ID di firma IPS e un tipo di query **All Matching Event Raw Messages**

sull'appliance Cisco Security MARS sarà disponibile un report che elenca gli incidenti creati dalla firma IPS.

- **NR-32719/00** per la firma IPS 32719/0
- **NR-33859/00** per la firma IPS 33859/00
- **NR-33860/0** per la firma IPS 33860/0
- **NR-3860/1** per la firma IPS 3860/1
- **NR-33861** per le firme IPS da 33861/0 a 33861/4

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 verranno visualizzati come tipo di evento sconosciuto 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

Cronologia delle revisioni

Revisione 1.1	25 febbraio 2011	Aggiornato per includere informazioni sul Signature ID 3861-0.
Revisione 1.0	23 febbraio	Pubblicazione iniziale.

	2011	

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

- Cisco TelePresence Hardening Guide
- Bollettini sulla mitigazione applicata da Cisco
- Cisco Security
- Servizio Cisco Security IntelliShield Alert Manager
- Guida Cisco per fortificare i dispositivi Cisco IOS
- Informazioni sui vettori di minaccia XSS (Cross-Site Scripting)
- 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
- Identificazione e mitigazione degli attacchi TTL in scadenza
- Un approccio orientato alla sicurezza per l'indirizzamento IP
- Protezione della lingua dei comandi degli strumenti su Cisco IOS
- Prodotti Cisco Firewall - Home Page su Cisco.com
- Documentazione del modulo Cisco ACE Application Control Engine
- Miglioramenti unicast Reverse Path Forwarding per il provider di servizi Internet
- Cisco Intrusion Prevention System
- Download di firme IPS Cisco
- Pagina di ricerca delle firme IPS Cisco
- Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco
- Vulnerabilità ed esposizioni comuni (CVE)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).