Identificazione e mitigazione dello sfruttamento dell'interfaccia di query aperte in Cisco Unified Communications Manager e Presence Server

Identificazione e mitigazione dello sfruttamento dell'interfaccia di query aperte in Cisco Unified Communications Manager e Presence Server

Codice identificativo: cisco-amb-20110824-cucm-cups

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110824-cucm-cups

Revisione 1.0

Per la Pubblica Release 2011 Agosto 24 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Questo bollettino sulla mitigazione applicata è un documento complementare all'*interfaccia open query di* PSIRT Security Advisory *in Cisco Unified Communications Manager e Presence Server* e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

Cisco Unified Communications Manager (CUCM) e Cisco Unified Presence Server (CUPS) contengono una vulnerabilità aperta dell'interfaccia di query SQL. 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 attraverso i pacchetti HTTPS che usano le porte TCP 443 e TCP 8443.

A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-1643.

Panoramica delle tecniche di mitigazione

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

Il software Cisco IOS può essere uno strumento efficace per prevenire gli attacchi tramite gli Access Control List (tACL) di transito.

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

Un'efficace prevenzione degli attacchi può essere fornita anche da Cisco ASA serie 5500 Adaptive Security Appliance e dal Firewall Services Module (FWSM) per gli switch Cisco Catalyst serie 6500 e i router Cisco serie 7600 che utilizzano gli ACL.

Questo meccanismo di protezione filtra e scarta i 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 FWSM possono fornire visibilità attraverso i messaggi syslog e i valori dei contatori visualizzati nell'output dei comandi **show**.

Gestione dei rischi

Si consiglia alle organizzazioni di seguire i processi standard di valutazione e mitigazione dei rischi per determinare l'impatto potenziale di [questa vulnerabilità|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

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

Attenuazione: Access Control List transit

Per proteggere la rete dal traffico che entra nei punti di accesso in entrata, che possono includere punti di connessione Internet, punti di connessione fornitori e partner o punti di connessione VPN, si consiglia agli amministratori di distribuire elenchi di controllo di accesso in transito (tACL) per applicare le policy. Gli amministratori possono costruire un ACL autorizzando esplicitamente solo il traffico autorizzato ad accedere alla rete dai punti di accesso in entrata o autorizzando il traffico autorizzato a transitare sulla rete in base alle configurazioni e ai criteri di sicurezza esistenti. La soluzione tACL non è in grado di fornire una protezione completa da questa vulnerabilità quando l'attacco proviene da un indirizzo di origine attendibile.

Il criterio ACL nega i pacchetti HTTPS non autorizzati sulla porta TCP 443 e sulla porta TCP 8443 che vengono 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 ports
! access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443 access-
list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443 !
!-- The following vulnerability-specific access control entries
!-- (ACEs) can aid in identification of attacks
! access-list 150 deny tcp any 192.168.60.0 0.0.0.255 eq 443 access-list 150 deny tcp
any 192.168.60.0 0.0.0.255 eq 8443 !
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Explicit deny for all other IP traffic
! access-list 150 deny ip any any !
!-- Apply tACL to interfaces in the ingress direction
! interface GigabitEthernet0/0 ip access-group 150 in
```

L'applicazione di un filtro con un elenco degli accessi all'interfaccia determinerà la trasmissione di messaggi ICMP "destinazione irraggiungibile" alla sorgente del traffico filtrato. La generazione di questi messaggi potrebbe avere l'effetto indesiderato di aumentare l'utilizzo della CPU sul dispositivo. Per impostazione predefinita, nel software Cisco IOS la generazione di pacchetti ICMP "destinazione irraggiungibile" è limitata a un pacchetto ogni 500 millisecondi. La generazione di messaggi ICMP "destinazione irraggiungibile" può essere disabilitata usando il comando di configurazione interfaccia **no ip unreachables**. La limitazione della velocità non raggiungibile ICMP può essere modificata dal valore predefinito utilizzando il comando di configurazione globale **ip icmp rate-limit unreachable** *interval-in-ms*.

Identificazione: Access Control List transit

Dopo che l'amministratore ha applicato l'ACL a un'interfaccia, il comando **show ip access-lists** restituisce il numero di pacchetti HTTPS sulla porta TCP 443 e sulla porta TCP 8443 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 esempio di output per **show ip access-lists 150**:

```
router#show ip access-lists 150
Extended IP access list 150
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 8443
    30 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (12 matches)
    40 deny tcp any 192.168.60.0 0.0.0.255 eq 8443 (26 matches)
    50 deny ip any any
router#
```

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

- **12** pacchetti **HTTPS** sulla **porta TCP 443** per la linea ACE 30
- **26** pacchetti **HTTPS** sulla **porta TCP 8443** per la linea ACE 40

Per ulteriori informazioni sull'analisi degli incidenti tramite i contatori ACE e gli eventi syslog, consultare il white paper sull'identificazione degli incidenti tramite il firewall e gli eventi syslog del router IOS Application Intelligence.

Gli amministratori possono utilizzare Embedded Event Manager per fornire strumentazione quando vengono soddisfatte condizioni specifiche, ad esempio accessi al contatore ACE. Il white paper sull'intelligence applicata Embedded Event Manager in a Security Context fornisce ulteriori dettagli sull'utilizzo di questa funzionalità.

Identificazione: Registrazione elenco accessi

L'opzione **log** e **log-input** access control list (ACL) causerà la registrazione dei pacchetti che corrispondono ad ACE specifici. L'opzione **log-input** abilita la registrazione dell'interfaccia in entrata, oltre agli indirizzi IP di origine e destinazione dei pacchetti e alle porte.

Attenzione: la registrazione dell'elenco di controllo di accesso può richiedere un utilizzo intensivo della CPU e deve essere utilizzata con estrema cautela. I fattori che determinano l'impatto della registrazione ACL sulla CPU sono la generazione di log, la trasmissione di log e la commutazione di processo per inoltrare i pacchetti che corrispondono alle voci ACE abilitate per il log.

Per il software Cisco IOS, il comando **ip access-list logging interval** *in-ms* può limitare gli effetti della commutazione di processo indotta dalla registrazione ACL. Il comando **logging rate-limit** *rate-per-second* [**except** *loglevel*] limita l'impatto della generazione e della trasmissione del log.

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

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

Cisco IOS NetFlow

Identificazione: Identificazione del flusso di traffico mediante i record NetFlow

Gli amministratori possono configurare Cisco IOS NetFlow sui router e gli switch Cisco IOS per

aiutare a identificare i flussi di traffico che potrebbero essere tentativi di sfruttare la vulnerabilità. Si consiglia agli amministratori di analizzare i flussi per determinare se si tratta di tentativi di sfruttare la vulnerabilità o se si tratta di flussi di traffico legittimi.

```
router#show ip cache flow
IP packet size distribution (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

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

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

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0 192.168.10.201 Gi0/1 192.168.60.102 06 0984 01BB 8
Gi0/0 192.168.11.54 Gi0/1 192.168.60.158 06 0911 20FB 2
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA     2
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   11 0B3E 00A1     4
Gi0/0 192.168.10.17 Gi0/1 192.168.60.97 06 0B89 20FB 3
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B     2
Gi0/0 192.168.12.185 Gi0/1 192.168.60.239 06 0BD7 01BB 8
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 HTTPS sulla porta **TCP 443 (valore esadecimale 01BB)** e sulla porta **TCP 8443 (valore esadecimale 20FB)**.

Per visualizzare solo i flussi di traffico per i pacchetti HTTPS sulla porta TCP 443 (valore esadecimale 01BB) e sulla porta TCP 8443 (valore esadecimale 20FB), eseguire il comando **show ip cache flow | include SrcIf|_06_.*(01BB|20FB)_** visualizzerà i record TCP NetFlow correlati, come mostrato di seguito:

Flussi TCP

```
router#show ip cache flow | include SrcIf|_06_.*(01BB|20FB)_
SrcIf         SrcIPaddress     DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0 192.168.12.110 Gi0/1 192.168.60.163 06 092A 01BB 6
Gi0/0 192.168.11.230 Gi0/1 192.168.60.20 06 0C09 01BB 1
Gi0/0 192.168.11.131 Gi0/1 192.168.60.245 06 0B66 20FB 18
Gi0/0 192.168.13.7 Gi0/1 192.168.60.162 06 0914 01BB 1
Gi0/0 192.168.41.86 Gi0/1 192.168.60.27 06 0B7B 20FB 2
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 HTTPS non autorizzati sulla porta TCP 443 e sulla porta TCP 8443 che vengono 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 ports
! 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 8443 !
!-- 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 443
access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 8443 !
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Explicit deny for all other IP traffic
! access-list tACL-Policy extended deny ip any any !
!-- Apply tACL to interface(s) in the ingress direction
! access-group tACL-Policy in interface outside
```

Identificazione: Access Control List transit

Dopo aver applicato l'ACL a un'interfaccia, gli amministratori possono usare il comando **show access-list** per identificare il numero di pacchetti HTTPS sulla porta TCP 443 e sulla porta TCP 8443 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; 5 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq https (hitcnt=5)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq 8443 (hitcnt=42)
access-list tACL-Policy line 3 extended deny tcp any
     192.168.60.0 255.255.255.0 eq https (hitcnt=20)
access-list tACL-Policy line 4 extended deny tcp any
     192.168.60.0 255.255.255.0 eq 8443 (hitcnt=17)
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=8)
firewall#
```

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

- **20** pacchetti **HTTPS** sulla **porta TCP 443** per la linea ACE 3
- **17** pacchetti **HTTPS** sulla **porta TCP 8443** per la linea ACE 4

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
  Aug 24 2011 00:08:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/443 by access-group "tACL-Policy"
  Aug 24 2011 00:08:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/443 by access-group "tACL-Policy"
  Aug 24 2011 00:08:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
         dst inside:192.168.60.240/8443 by access-group "tACL-Policy"
  Aug 24 2011 00:08:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
         dst inside:192.168.60.115/8443 by access-group "tACL-Policy"
  Aug 24 2011 00:08:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
         dst inside:192.168.60.38/443 by access-group "tACL-Policy"
  Aug 24 2011 00:08:13: %ASA-4-106023: Deny tcp src outside:192.0.2.175/2950
         dst inside:192.168.60.250/443 by access-group "tACL-Policy"
firewall#
```

Nell'esempio precedente, i messaggi registrati per il *tACL-Policy* tACL mostrano i pacchetti **HTTPS** per la **porta TCP 443** e la **porta TCP 8443** 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.

Ulteriori informazioni

IL PRESENTE DOCUMENTO VIENE FORNITO "COSÌ COM'È" E NON IMPLICA ALCUNA GARANZIA O CONCESSIONE, INCLUSE LE GARANZIA DI COMMERCIABILITÀ O IDONEITÀ PER UNO SCOPO SPECIFICO. L'UTILIZZO DA PARTE DELL'UTENTE DELLE INFORMAZIONI CONTENUTE NEL DOCUMENTO O NEI MATERIALI ACCESSIBILI DAL DOCUMENTO AVVIENE A PROPRIO RISCHIO. CISCO SI RISERVA IL DIRITTO DI MODIFICARE O AGGIORNARE IL PRESENTE DOCUMENTO IN QUALSIASI MOMENTO.

Cronologia delle revisioni

Revisione 1.0	2011-AGOSTO-24	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
- 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).