Identificazione e mitigazione dell'utilizzo delle credenziali predefinite per l'account root su Cisco Media Experience Engine 5600

Identificazione e mitigazione dell'utilizzo delle credenziali predefinite per l'account root su Cisco Media Experience Engine 5600

ID advisory: cisco-amb-20110601-mxe

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110601-mxe

Revisione 1.0

Per la Pubblica Release 2011 1 Giugno 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Questo bollettino sulla mitigazione applicata è un documento complementare alle *credenziali predefinite di* PSIRT Security Advisory *per l'account root su Cisco Media Experience Engine 5600* e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

Cisco Media Experience Engine (MXE) 5600 contiene un account amministratore *radice* abilitato per impostazione predefinita con una password predefinita. 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 o la divulgazione di 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 SSH che usano la porta TCP 22 e i pacchetti Telnet che usano la porta TCP 23. Nota: Telnet è disabilitato per

impostazione predefinita su Cisco MXE 5600 ma può essere utilizzato come vettore di utilizzo se abilitato manualmente sui dispositivi interessati.

A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2011-1623.

Le informazioni sul software vulnerabile, non interessato e fisso sono disponibili in PSIRT Security Advisory, disponibile al seguente collegamento: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110601-mxe.

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 iACL (Access Control List) dell'infrastruttura. Questo meccanismo di protezione filtra e scarta i pacchetti che stanno tentando di sfruttare questa vulnerabilità.

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

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

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

Il software Cisco IOS e i firewall 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

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

Mitigazione e identificazione specifiche del dispositivo

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

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

- Router e switch Cisco IOS
- Cisco IOS NetFlow
- Cisco ASA e firewall FWSM

Router e switch Cisco IOS

Mitigazione: Access Control List Dell'Infrastruttura

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

Il criterio iACL nega i pacchetti SSH non autorizzati sulla porta TCP 2 e i pacchetti Telnet sulla porta TCP 23 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. 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 22
permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 23 ! !-- 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 22 deny tcp any 192.168.60.0
0.0.0.255 eq 23 ! !-- 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 dal valore predefinito utilizzando il comando di configurazione globale **ip icmp rate-limit unreachable** *interval-in-ms*.

Identificazione: Access Control List dell'infrastruttura

Dopo che l'amministratore ha applicato l'iACL a un'interfaccia, il comando **show ip access-lists** restituisce il numero di pacchetti SSH sulla porta TCP 22 e di pacchetti Telnet sulla porta TCP 23 che sono stati filtrati sulle interfacce a cui è applicato l'iACL. Gli amministratori devono esaminare i pacchetti filtrati per determinare se sono tentativi di sfruttare questa vulnerabilità. Di seguito è riportato un esempio di output per **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 ssh
    20 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq telnet
    30 deny tcp any 192.168.60.0 0.0.0.255 eq ssh (23 matches)
    40 deny tcp any 192.168.60.0 0.0.0.255 eq telnet (17 matches)
    50 deny ip any 192.168.60.0 0.0.0.255
router#
```

Nell'esempio precedente, l'elenco degli accessi Infrastructure-ACL-Policy ha scartato 23 pacchetti SSH sulla porta TCP 22 per la voce dell'elenco di controllo degli accessi (ACE), linea 30, e 17 pacchetti Telnet sulla porta **TCP 23** 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.

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 (2409 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .349 .650 .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
  89 active, 4007 inactive, 318 added
```

```
  4544 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             38      0.0         9    40      0.0       0.0      15.2
TCP-other          108      0.0         6    40      0.0       0.0      15.5
UDP-TFTP            10      0.0         4    28      0.0       0.0      15.7

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
UDP-other           73      0.0         7    28      0.0       0.0      15.5
Total:             229      0.0         7    35      0.0       0.0      15.5

SrcIf         SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.74.110  Et0/1          192.168.13.20   06 C8A7 D4BE     5
Et0/0         192.168.23.20   Et0/1          192.168.226.172 11 2123 540A     1
Et0/0         192.168.53.205  Et0/1          192.168.60.88   11 DEB7 0045     5
Et0/0         192.168.0.115   Et0/1          192.168.60.214  06 F73A 0050    11
Et0/0         192.168.0.30    Et0/1          192.168.60.63   06 A64E 0016     3
Et0/0         192.168.211.52  Et0/1          192.168.113.252 11 17AA 8F11    17
Et0/0         192.168.34.222  Et0/1          192.168.58.190  11 9A8F 2AD3     5
Et0/0         192.168.198.3   Et0/1          192.168.60.104  11 4F4D 0045     1
Et0/0         192.168.240.90  Et0/1          192.168.88.197  06 3D88 0017    15
Et0/0         192.168.0.96    Et0/1          192.168.60.126  06 9621 0017     3
Et0/0         192.168.155.22  Et0/1          192.168.80.13   06 1298 EB6A    10
Et0/0         192.168.0.20    Et0/1          192.168.60.78   06 1541 0050     3
Et0/0         192.168.0.2     Et0/1          192.168.60.195  06 5419 01BB     5
Et0/0         192.168.223.127 Et0/1          192.168.121.153 06 0613 17E5     7
Et0/0         192.168.0.28    Et0/1          192.168.60.101  06 B5C6 0017     2
Et0/0         192.168.92.207  Et0/1          192.168.43.167  11 1FF5 2815    11
Et0/0         192.168.0.28    Et0/1          192.168.60.139  06 24E9 0050     6
Et0/0         192.168.122.182 Et0/1          192.168.68.21   11 71C2 80BB    11
Et0/0         192.168.18.228  Et0/1          192.168.203.86  11 0630 77B4    16
Et0/0         192.168.0.218   Et0/1          192.168.60.248  06 531B 01BB    15
Et0/0         192.168.26.81   Et0/1          192.168.213.193 06 76D9 11B0     3
Et0/0         192.168.225.144 Et0/1          192.168.28.79   11 FF8F 299D    32
Et0/0         192.168.166.100 Et0/1          192.168.60.217  11 0B47 0045    10
Et0/0         192.168.49.15   Et0/1          192.168.139.203 11 D880 6D41     4
Et0/0         192.168.0.120   Et0/1          192.168.60.41   06 D24F 0016     6
Et0/0         192.168.0.109   Et0/1          192.168.60.189  06 B0B0 0016    11
Et0/0         192.168.0.65    Et0/1          192.168.60.136  06 6110 01BB     2
Et0/0         192.168.0.51    Et0/1          192.168.60.43   06 4090 0050    17
Et0/0         192.168.160.238 Et0/1          192.168.38.104  06 F54E DEE1    14
router#
```

Nell'esempio precedente, sono presenti più flussi per SSH sulla porta TCP 22 (valore esadecimale 0016) e **Telnet** sulla porta **TCP 23 (valore esadecimale 0017)**.

Per visualizzare solo i flussi di traffico per i pacchetti SSH sulla porta TCP 2 (valore esadecimale 0016) e i pacchetti Telnet sulla porta TCP 23 (valore esadecimale 0017), usare il comando **show ip cache flow | include SrcIf|**_06_.*0016|0017 visualizzerà i record TCP NetFlow correlati, come mostrato di seguito:

Flussi TCP

```
router#show ip cache flow | include SrcIf|_06_.*0016|0017
SrcIf         SrcIPaddress     DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.0.30     Et0/1          192.168.60.63   06 A64E 0016     3
Et0/0         192.168.0.120    Et0/1          192.168.60.41   06 D24F 0017     6
Et0/0         192.168.0.109    Et0/1          192.168.60.189  06 B0B0 0016    11
router#
```

Cisco ASA e firewall FWSM

Attenuazione: Access Control List transit

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

Il criterio ACL nega i pacchetti SSH non autorizzati sulla porta TCP 2 e i pacchetti Telnet sulla porta TCP 23 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 22 access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 23 ! !-- 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
22 access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq 23 !
!-- 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 SSH sulla porta TCP 22 e di pacchetti Telnet sulla porta TCP 23 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 ssh (hitcnt=485)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1
  192.168.60.0 255.255.255.0 eq telnet (hitcnt=29)
access-list tACL-Policy line 3 extended deny tcp any
  192.168.60.0 255.255.255.0 eq ssh (hitcnt=58)
access-list tACL-Policy line 4 extended deny tcp any
  192.168.60.0 255.255.255.0 eq telnet (hitcnt=16)
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=8)
firewall#
```

Nell'esempio precedente, il criterio tACL dell'elenco degli accessi ha scartato **58** pacchetti **SSH** sulle **porte TCP 22** e **16** pacchetti Telnet sulla **porta TCP 23** ricevuti da un host o da una rete non attendibile. Inoltre, il messaggio syslog *106023* può fornire informazioni preziose, tra cui l'indirizzo IP di origine e di destinazione, i numeri di porta di origine e di destinazione e il protocollo IP per il pacchetto rifiutato.

Identificazione: Messaggi syslog elenco accessi firewall

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

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

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

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

```
firewall#show logging | grep 106023
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.194/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.164/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.106/23 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.1/1025
 dst inside:192.168.60.241/23 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.169/1025
 dst inside:192.168.60.56/22 by access-group "tACL-Policy"
Jun 1 2011 07:32:32: %ASA-4-106023: Deny tcp src outside:192.0.2.36/1025
 dst inside:192.168.60.202/22 by access-group "tACL-Policy"
firewall#
```

Nell'esempio precedente, i messaggi registrati per il tACL-Policy mostrano i pacchetti **SSH** per la **porta TCP 22** e i pacchetti **Telnet** per la **porta TCP 23** inviati al blocco di indirizzi assegnato ai dispositivi dell'infrastruttura.

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-Giugno-01	Versione pubblica iniziale

Procedure di sicurezza di Cisco

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

Informazioni correlate

- Bollettini sulla mitigazione applicata da Cisco
- Cisco Security
- Servizio Cisco Security IntelliShield Alert Manager
- Guida Cisco per fortificare i dispositivi Cisco IOS
- Cisco IOS NetFlow - Home Page su Cisco.com
- White paper su Cisco IOS NetFlow
- Analisi delle prestazioni di NetFlow
- White paper su Cisco Network Foundation Protection
- Presentazioni di Cisco Network Foundation Protection
- Identificazione e mitigazione degli attacchi TTL in scadenza
- Un approccio orientato alla sicurezza per l'indirizzamento IP
- Contromisure per l'utilizzo dannoso delle intestazioni di routing IPv6 di tipo 0
- Protezione della lingua dei comandi degli strumenti su Cisco IOS
- 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).