Identificazione e mitigazione dello sfruttamento della vulnerabilità nei servizi comuni di CiscoWorks

Identificazione e mitigazione dello sfruttamento della vulnerabilità nei servizi comuni di CiscoWorks

ID advisory: cisco-amb-20101027-cs

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20101027-cs

Revisione 1.0

Per la Pubblica Release 2010 Ottobre 27 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Questo bollettino sulla mitigazione applicata è un documento complementare all'advisory della sicurezza PSIRT *CiscoWorks Common Services Arbitrary Code Execution Vulnerability* e fornisce tecniche di identificazione e mitigazione che gli amministratori possono distribuire sui dispositivi di rete Cisco.

Caratteristiche di vulnerabilità

Cisco Common Services per CiscoWorks contiene una vulnerabilità quando elabora un pacchetto in formato non corretto. Questa vulnerabilità può essere sfruttata in remoto senza autenticazione e senza l'interazione dell'utente finale. L'utilizzo di questa vulnerabilità può consentire l'esecuzione arbitraria del codice o causare l'arresto anomalo del dispositivo interessato. Il vettore di attacco per l'utilizzo avviene attraverso i pacchetti che usano la porta TCP 443 e la porta TCP 1741 quando viene usata la configurazione predefinita.

A questa vulnerabilità è stato assegnato l'identificatore CVE CVE-2010-3036.

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-20101027-cs.

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.

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

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

Il software Cisco IOS, Cisco ASA, i firewall FWSM, l'appliance e il modulo Cisco ACE Application Control Engine possono fornire visibilità attraverso i messaggi syslog e i valori dei contatori visualizzati nell'output dei comandi **show**.

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

Gestione dei rischi

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

Mitigazione e identificazione specifiche del dispositivo

Attenzione: l'efficacia di qualsiasi tecnica di mitigazione dipende dalle situazioni specifiche del

cliente, come il mix di prodotti, la topologia di rete, il comportamento del traffico e la missione organizzativa. Come per qualsiasi modifica apportata alla configurazione, valutare l'impatto della configurazione prima di applicare la modifica.

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

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

Router e switch Cisco IOS

Attenuazione: Access Control List transit

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

Il criterio ACL nega l'invio ai dispositivi interessati di pacchetti non autorizzati sulle porte predefinite, la porta TCP 443 e la porta TCP 1741. 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 1741 ! !-- 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 1741 ! !--
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 sulle porte TCP 443 e TCP 1741 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 1741
    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 1741 (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 sulla **porta TCP 443** per la linea ACE 30
- **26** pacchetti sulla **porta TCP 1741** 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 (17258967 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .013 .225 .422 .155 .035 .008 .005 .004 .002 .001 .014 .002 .002 .003 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .045 .017 .034 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  18 active, 65518 inactive, 2445817 added
  226043591 ager polls, 0 flow alloc failures
  Active flows timeout in 2 minutes
  Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 533256 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         653      0.0        77    40      0.0      27.4      24.0
TCP-FTP            765      0.0        15    42      0.0       1.3      25.8
TCP-FTPD             3      0.0       324   608      0.0       1.9      42.9
TCP-WWW          43844      0.0        20   456      0.2       9.3      40.0
TCP-SMTP          4973      0.0         6    59      0.0      35.3      59.7
TCP-X                2      0.0         1    52      0.0       0.0      66.8
TCP-BGP              2      0.0         1    52      0.0       0.0      63.7
TCP-NNTP             2      0.0         1    52      0.0       0.0      88.7
TCP-other       276300      0.0        19   267      1.2      29.1      41.8
UDP-DNS         236963      0.0         2    69      0.1       8.8      57.8
UDP-NTP          31121      0.0         1    75      0.0       0.2      60.3
UDP-TFTP             9      0.0         4    80      0.0      27.6      55.7
UDP-other       485427      0.1         8   106      0.9      21.6      56.4
ICMP            642287      0.1         2    83      0.3      10.6      60.0
IGMP            265863      0.0         2    37      0.1      53.9      42.7
IP-other        457584      0.1         8    92      0.9      94.0      16.3
Total:         2445798      0.5         7   167      4.0      34.9      46.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.137.50  Gi0/1         192.168.60.42   11 0984 00A1     1
Gi0/0         192.168.211.3   Gi0/1         192.168.60.101  11 0911 00A1     3
Gi0/0         192.168.18.79   Gi0/1         192.168.60.105  06 1C16 06CD     4
Gi0/0         192.168.203.49  Gi0/1         192.168.60.67   11 0B3E 00A1     5
```

```
Gi0/0          192.168.101.251 Gi0/1          192.168.60.103   06 3A89 01BB     1
Gi0/0          192.168.122.5   Gi0/1          192.168.60.29    11 0BD7 00A1     1
Gi0/0          192.168.40.131  Gi0/1          192.168.60.80    06 22FC 01BB     7
router#
```

Nell'esempio precedente, sono presenti più flussi sulla porta **TCP 443 (valore esadecimale 01BB)** e sulla porta **TCP 1741 (valore esadecimale 06CD)**.

Per visualizzare solo i flussi di traffico per i pacchetti sulla porta TCP 443 (valore esadecimale 01BB) e sulla porta TCP 1741 (valore esadecimale 06CD), eseguire il comando **show ip cache flow | include SrcIf|**_06_.*(01BB|06CD)_visualizzerà i record TCP NetFlow correlati, come mostrato di seguito:

Flussi TCP

```
router#show ip cache flow | include SrcIf|_06_.*(01BB|06CD)_
SrcIf          SrcIPaddress     DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0          192.168.18.79    Gi0/1          192.168.60.105  06 1C16 06CD     4
Gi0/0          192.168.101.251  Gi0/1          192.168.60.103  06 3A89 01BB     1
Gi0/0          192.168.40.131   Gi0/1          192.168.60.80   06 22FC 01BB     7
router#
```

Cisco ASA e firewall FWSM

Attenuazione: Access Control List transit

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

Il criterio ACL nega l'invio ai dispositivi interessati di pacchetti non autorizzati sulle porte predefinite, la porta TCP 443 e la porta TCP 1741. 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 https access-list tACL-Policy extended
permit tcp host 192.168.100.1 192.168.60.0 255.255.255.0 eq 1741 ! !-- 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
https access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq
1741 ! !-- 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 sulle porte TCP 443 e TCP 1741 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=0)
access-list tACL-Policy line 2 extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 1741 (hitcnt=0)
access-list tACL-Policy line 3 extended deny tcp any 192.168.60.0 255.255.255.0 eq
https (hitcnt=15)
access-list tACL-Policy line 4 extended deny tcp any 192.168.60.0 255.255.255.0 eq
1741 (hitcnt=7)
access-list tACL-Policy line 5 extended deny ip any any (hitcnt=0)
```

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

- **15** pacchetti sulla **porta TCP 443** per la linea ACE 3
- **7** pacchetti sulla **porta TCP 1741** 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
  Oct 21 2010 00:07:23: %ASA-4-106023: Deny tcp src outside:192.0.2.101/3710
         dst inside:192.168.60.112/1741 by access-group "tACL-Policy"
  Oct 21 2010 00:07:24: %ASA-4-106023: Deny tcp src outside:192.0.2.98/3711
```

```
        dst inside:192.168.60.27/443 by access-group "tACL-Policy"
  Oct 21 2010 00:07:24: %ASA-4-106023: Deny tcp src outside:192.0.2.149/3712
        dst inside:192.168.60.48/1741 by access-group "tACL-Policy"
  Oct 21 2010 00:07:24: %ASA-4-106023: Deny tcp src outside:192.0.2.172/3713
        dst inside:192.168.60.131/1741 by access-group "tACL-Policy"
  Oct 21 2010 00:07:24: %ASA-4-106023: Deny tcp src outside:192.0.2.129/3714
        dst inside:192.168.60.231/443 by access-group "tACL-Policy"
firewall#
```

Nell'esempio precedente, i messaggi registrati per il *tACL-Policy* mostrano i pacchetti per la **porta TCP 443** e la **porta TCP 1741** inviati al blocco di indirizzi assegnato ai dispositivi interessati.

Per ulteriori informazioni sui messaggi syslog per le appliance di sicurezza ASA, consultare la guida Cisco ASA serie 5500 System Log Messages, versione 8.2. Per ulteriori informazioni sui messaggi syslog per il modulo FWSM, consultare i messaggi log del sistema di registrazione dello switch Catalyst serie 6500 e del router Cisco serie 7600 Firewall Services Module.

Per ulteriori informazioni sull'analisi degli incidenti tramite eventi syslog, consultare il white paper Identificazione degli incidenti tramite firewall e eventi syslog del router IOS Applicati Intelligence.

Cisco Intrusion Prevention System

Attenuazione: azioni evento firma Cisco IPS

Gli amministratori possono utilizzare gli accessori e i moduli di servizi IPS (Cisco Intrusion Prevention System) per rilevare le minacce e contribuire a prevenire i tentativi di sfruttare la vulnerabilità descritta in questo documento. A partire dall'aggiornamento della firma S524 per i sensori con Cisco IPS versione 6.x e successive, la vulnerabilità può essere rilevata dalla firma 30859/0 (nome firma: CiscoWorks Common Services Arbitrary Code Execution Vulnerability). La firma 30859/0 è abilitata per impostazione predefinita, attiva un evento di *alta* gravità, ha un indice di fedeltà della firma (SFR) di 85 ed è configurata con un'azione evento predefinita di **produce-alert**.

La firma 30859/0 viene attivata quando viene rilevato un singolo pacchetto inviato tramite la porta TCP 1741. L'attivazione di questa firma può indicare un potenziale utilizzo della vulnerabilità.

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

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

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

Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco

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

L'appliance Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) può creare incidenti relativi a eventi correlati alla vulnerabilità descritta in questo documento utilizzando la firma IPS 30859/0 (nome firma: Vulnerabilità CiscoWorks Common Services Arbitrary Code Execution). Dopo aver scaricato l'aggiornamento della firma dinamica S524, utilizzando la parola chiave **NR-30859/0** per la firma IPS 30859/0 e un tipo di query **All Matching Events** (Tutti gli eventi corrispondenti) sull'accessorio Cisco Security MARS sarà disponibile un report in cui sono elencati gli incidenti creati dalla firma IPS.

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

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

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

```
System Rule: CS-MARS IPS Signature Update Failure
```

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

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

Ulteriori informazioni

Cronologia delle revisioni

Revisione 1.0	27 ottobre 2010	Versione pubblica iniziale

Procedure di sicurezza di Cisco

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

Informazioni correlate

- Bollettini sulla mitigazione applicata da Cisco
- Cisco Security
- Servizio Cisco Security IntelliShield Alert Manager
- Guida Cisco per fortificare i dispositivi Cisco IOS
- Cisco IOS NetFlow - Home Page su Cisco.com
- White paper su Cisco IOS NetFlow
- Analisi delle prestazioni di NetFlow
- White paper su Cisco Network Foundation Protection
- Presentazioni di Cisco Network Foundation Protection
- Un approccio orientato alla sicurezza per l'indirizzamento IP
- Prodotti Cisco Firewall - Home Page su Cisco.com
- Cisco Intrusion Prevention System
- Download di firme IPS Cisco
- Pagina di ricerca delle firme IPS Cisco
- Sistema di monitoraggio, analisi e risposta per la sicurezza Cisco
- Vulnerabilità ed esposizioni comuni (CVE)

Informazioni su questa traduzione

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