Identificazione e mitigazione dello sfruttamento della vulnerabilità dell'overflow dell'heap del codificatore di entità HTML PHP in più interfacce di gestione basate sul Web

Identificazione e mitigazione dello sfruttamento della vulnerabilità dell'overflow dell'heap del codificatore di entità HTML PHP in più interfacce di gestione basate sul Web

ID advisory: cisco-amb-20070425-http

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070425-http

Revisione 1.0

Per la Pubblica Release 2007 Aprile 25 16:00 UTC (GMT)

Sommario

Risposta di Cisco

Questo bollettino sulla mitigazione applicata è un documento complementare alla risposta di sicurezza PSIRT: Vulnerabilità dell'overflow dell'heap del codificatore di entità HTML PHP in più interfacce di gestione basate su Web. Documenta ulteriori tecniche di mitigazione che possono essere implementate sui dispositivi Cisco all'interno della rete.

Caratteristiche di vulnerabilità

Una vulnerabilità esiste in alcune funzioni PHP incluse in prodotti Cisco specifici. Un utente malintenzionato autenticato può sfruttare questa vulnerabilità in remoto. Non è necessaria alcuna interazione da parte dell'utente. L'utilizzo riuscito di questa vulnerabilità può consentire

l'esecuzione di codice senza privilegi. I vettori utilizzati per sfruttare questa vulnerabilità sono i protocolli HTTP e HTTPS (porte TCP 80 e 443). Questa vulnerabilità è coperta da CVE ID 2006-5465.

Informazioni sul software vulnerabile, non interessato e fisso sono disponibili nella risposta di sicurezza PSIRT all'indirizzo https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070425-http

Panoramica delle tecniche di mitigazione

I dispositivi Cisco forniscono diverse contromisure per la vulnerabilità dell'overflow dell'heap del codificatore di entità HTML PHP. Molti di questi metodi di protezione dovrebbero essere considerati come best practice generali di sicurezza per i dispositivi dell'infrastruttura e il traffico che attraversa la rete.

Il software Cisco IOS può essere uno strumento efficace per prevenire gli attacchi tramite gli iACL (Access Control List) dell'infrastruttura. I firewall Cisco ASA, PIX e Firewall Services Module (FWSM) possono anche fornire mezzi efficaci di prevenzione degli attacchi tramite gli Access Control List (tACL) di transito. Sia l'infrastruttura che gli Access Control List (ACL) di transito filtrano ed eliminano (scartano) l'indirizzo IP di origine dei pacchetti che stanno cercando di sfruttare la vulnerabilità descritta in questo documento.

I controlli di rilevamento possono essere eseguiti da Cisco IOS NetFlow con i record di flusso e dal software Cisco IOS, da Cisco ASA serie 5500 Adaptive Security Appliance, Cisco PIX serie 500 Security Appliance e FWSM per gli switch Cisco Catalyst serie 6500 e i router Cisco serie 7600 tramite messaggi syslog e i valori dei contatori visualizzati nell'output dei comandi **show**.

Gestione dei rischi

Le organizzazioni devono seguire il processo standard di attenuazione dei rischi per determinare l'impatto potenziale di questa vulnerabilità. I documenti che possono essere utilizzati per aiutare nella valutazione dei rischi sono disponibili in Triage dei rischi per la sicurezza Annunci di vulnerabilità e Triage dei rischi e Prototyping.

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.

Informazioni specifiche sulla mitigazione e l'identificazione sono disponibili per i seguenti dispositivi:

- Router Cisco IOS
- Cisco IOS NetFlow
- Cisco ASA, PIX e firewall FWSM

Router Cisco IOS

Mitigazione: Access Control List Dell'Infrastruttura

Al fine di proteggere i dispositivi dell'infrastruttura e ridurre al minimo i rischi, l'impatto e l'efficacia degli attacchi diretti all'infrastruttura, è necessario implementare gli elenchi di controllo di accesso all'infrastruttura iACL per applicare la policy sul traffico inviato alle apparecchiature 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 devono essere applicati in direzione entrata a tutte le interfacce su cui è stato configurato un indirizzo IP di layer 3.

Nell'esempio seguente, il blocco di indirizzi 192.168.1.0/24 è lo spazio di indirizzi dell'infrastruttura. Il criterio iACL nega i pacchetti HTTP e HTTPS destinati alle porte TCP 80 e 443 e inviati agli indirizzi che fanno parte dello spazio degli indirizzi dell'infrastruttura. È necessario prestare attenzione a consentire il traffico richiesto per il routing e l'accesso amministrativo prima di rifiutare tutto il traffico inviato direttamente ai dispositivi dell'infrastruttura. 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.

Le voci di controllo di accesso (ACE, Access Control Entry) aggiunte devono essere implementate come parte di un criterio iACL utilizzato per filtrare il traffico ai punti di ingresso della rete.

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
!-- Permit additional Layer 3 and Layer 4 traffic destined for infrastructure !--
address space as dictated by existing security policies and configurations. ! !--
Permit/deny traffic to infrastructure IP addresses in accordance !-- with security
policy. ! !-- Vulnerability-specific deny statements to aid identification deny tcp
any 192.168.1.0 0.0.0.255 eq 80 deny tcp any 192.168.1.0 0.0.0.255 eq 443 !-- Default
deny to affected IP addresses deny ip any 192.168.1.0 0.0.0.255 !-- Permit/deny all
other IP traffic in accordance with !-- existing security policies and
configurations. ! !-- Apply iACL to interface(s) 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. Ciò potrebbe avere l'effetto indesiderato di aumentare l'utilizzo della CPU perché il dispositivo di filtraggio deve generare questi messaggi ICMP "destinazione irraggiungibile". In 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 icmp unreachables**. La limitazione della velocità non raggiungibile ICMP può essere modificata dal valore predefinito di uno su 500 millisecondi usando il comando di configurazione globale **ip icmp rate-limit unreachable** *interval-in-ms*. Gli amministratori possono specificare intervalli da 1 a 4294967295 millisecondi.

Identificazione: Access Control List dell'infrastruttura

Con un iACL, dopo aver applicato l'elenco degli accessi a un'interfaccia nella direzione in entrata, il comando **show access-list** può essere usato per identificare il numero di pacchetti HTTP e

HTTPS sulle porte TCP 80 e 443 che vengono filtrati. I pacchetti filtrati devono essere esaminati per determinare se sono tentativi di sfruttare questa vulnerabilità. Di seguito è riportato un esempio di output per **show access-list infrastructure-acl-policy**:

```
router#show access-list infrastructure-acl-policy
Extended IP access list infrastructure-acl-policy
10 deny tcp any 192.168.1.0 0.0.0.255 eq 80 (92 matches)
20 deny udp any 192.168.1.0 0.0.0.255 eq 443 (23 matches)
30 deny ip any 192.168.1.0 0.0.0.255
-- Infrastructure ACL Policy Truncated --
router#
```

Nell'esempio precedente, l'elenco degli accessi *infrastruttura-acl-policy* ha scartato 92 pacchetti HTTP sulla porta TCP 80 per l'ID sequenza ACE 10 e 23 pacchetti HTTPS sulla porta TCP 443 per l'ID sequenza ACE 20. L'iACL viene applicato all'interfaccia Gigabit Ethernet0/0 in direzione di entrata.

Cisco IOS NetFlow

Identificazione: Identificazione del flusso di traffico mediante i record NetFlow

Cisco IOS NetFlow può essere configurato sui router e sugli switch Cisco IOS per aiutare a identificare i flussi di traffico che potrebbero essere tentativi potenziali di sfruttare la vulnerabilità descritta in questo documento. I pacchetti devono essere esaminati per determinare se sono tentativi di sfruttare questa vulnerabilità o traffico legittimo.

```
router#show ip cache flow
IP packet size distribution (149962503 total packets):
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.008 .582 .047 .008 .008 .008 .005 .012 .000 .001 .004 .001 .002 .002 .006
512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.001 .001 .161 .011 .122 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
27 active, 65509 inactive, 65326701 added
208920154 ager polls, 0 flow alloc failures
Active flows timeout in 1 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
27 active, 16357 inactive, 4854213 added, 4854213 added to flow
0 alloc failures, 0 force free
1 chunk, 11 chunks 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 11409641 2.6 1 49 3.1 0.0 1.5
TCP-FTP 7371 0.0 8 54 0.0 6.0 7.8
TCP-FTPD 713 0.0 3109 889 0.5 50.4 0.6
TCP-WWW 182891 0.0 13 735 0.5 4.3 9.3
TCP-SMTP 12 0.0 1 47 0.0 0.0 10.5
TCP-X 731 0.0 1 40 0.0 0.0 1.4
TCP-BGP 13 0.0 1 46 0.0 0.0 10.3
TCP-NNTP 12 0.0 1 47 0.0 0.0 9.7
TCP-Frag 70401 0.0 1 688 0.0 0.0 22.7
TCP-other 49417868 11.5 2 340 28.8 0.1 1.4
UDP-DNS 1411124 0.3 1 57 0.4 0.0 15.4
UDP-NTP 1365184 0.3 1 76 0.3 0.6 15.5
```

```
UDP-TFTP 10 0.0 2 57 0.0 6.6 18.6
UDP-other 1134163 0.2 2 160 0.5 0.3 16.6
ICMP 325667 0.0 7 48 0.5 11.7 20.0
IPv6INIP 15 0.0 1 1132 0.0 0.0 15.4
GRE 694 0.0 1 50 0.0 0.0 15.4
IP-other 2 0.0 2 20 0.0 0.1 15.7
Total: 65326512 15.2 2 315 34.9 0.1 2.4

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Gi0/0 10.21.96.74 Gi0/1* 192.168.1.11 06 F079 01BB 4
Gi0/0 10.21.96.74 Gi0/1 192.168.1.11 06 F079 01BB 4
Gi0/0 10.89.16.34 Gi0/1* 192.168.150.60 06 0FC8 0016 1
Gi0/0 10.89.16.34 Gi0/1 192.168.150.60 06 0FC8 0016 1
Gi0/1 192.168.150.60 Gi0/0* 10.89.16.34 06 0016 0FC8 1
Gi0/1 192.168.150.60 Gi0/0 10.89.16.34 06 0016 0FC8 1
Gi0/1 192.168.150.1 Gi0/0* 198.41.0.4 11 0401 0035 1
Gi0/1 192.168.150.1 Gi0/0 198.41.0.4 11 0401 0035 1
Gi0/0 192.168.208.63 Local 192.168.208.20 06 8876 0017 76
Gi0/1 192.168.128.2 Gi0/0* 10.88.226.1 11 007B 007B 1
Gi0/1 192.168.128.2 Gi0/0 10.88.226.1 11 007B 007B 1
Gi0/1 192.168.144.3 Gi0/0* 10.88.226.1 11 007B 007B 1
Gi0/1 192.168.144.3 Gi0/0 10.88.226.1 11 007B 007B 1
Gi0/0 10.88.226.1 Gi0/1* 192.168.144.3 11 007B 007B 1
Gi0/0 10.88.226.1 Gi0/1 192.168.144.3 11 007B 007B 1
Gi0/1 192.168.150.1 Gi0/0* 192.228.79.201 11 0401 0035 1
Gi0/1 192.168.150.1 Gi0/0 192.228.79.201 11 0401 0035 1
Gi0/1 192.168.150.1 Gi0/0* 128.63.2.53 11 0401 0035 1
Gi0/1 192.168.150.1 Gi0/0 128.63.2.53 11 0401 0035 1
```

Nell'esempio precedente, sono presenti più flussi per il protocollo HTTPS sulla porta 443 (valore esadecimale <01BB>). Il traffico proviene dalla versione 10.21.96.74 e viene inviato all'indirizzo 192.168.1.11, che viene utilizzato per i dispositivi dell'infrastruttura. Gli amministratori di rete possono utilizzare le istruzioni **include** per includere solo determinati indirizzi IP di destinazione o porte di destinazione per limitare l'output NetFlow ai dati che hanno maggiori probabilità di essere rilevanti. Un esempio potrebbe essere **show ip cache flow | includere 01BB**, che indica solo gli host per cui è in uso la porta TCP 443 (valore esadecimale <01BB>). È necessario esaminare questi flussi per determinare se provengono da host e/o reti non attendibili.

Cisco ASA, PIX e firewall FWSM

Attenuazione: Access Control List transit

Per proteggere la rete dal traffico ai margini che entra nella rete ai punti di accesso in entrata o al traffico che attraversa la rete, è necessario distribuire gli elenchi di controllo di accesso (tACL) di transito per applicare le policy al traffico. 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.

Nell'esempio seguente, il blocco di indirizzi 192.168.1.0/24 è lo spazio di indirizzi dell'infrastruttura. Il criterio ACL nega i pacchetti non autorizzati sulle porte TCP 80 (HTTP) e 443 (HTTPS) inviati agli indirizzi che fanno parte dello spazio degli indirizzi dell'infrastruttura

Ènecessario 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'installazione

dei tACL.

Ulteriori informazioni sugli ACL sono disponibili sul sito Access Control Lists: Filtering at Your Edge (Liste di controllo dell'accesso in transito: filtraggio sul perimetro della rete).

```
!-- Permit/Deny additional Layer 3 and Layer 4 traffic to enter !-- the network at
ingress access points or traffic that has been un/authorized !-- to transit the
network in accordance with existing security policies !-- and configurations. Deny
all !-- packets on TCP ports 80 and 443 sent to any IP address configured within the
!-- address block of 192.168.1.0/24, which is the infrastructure address !-- space,
except from known trusted source networks (ex: management networks, !-- security
operations center, network operations center). ! !-- The following are vulnerability-
specific access control entries (ACEs) to aid !-- in identification of attacks.
access-list transit-acl-policy extended deny tcp any 192.168.1.0 255.255.255.0 eq www
access-list transit-acl-policy extended deny tcp any 192.168.1.0 255.255.255.0 eq
https ! !-- Explicit default deny ACE for unauthorized traffic entering the network
!-- at ingress access points or unauthorized transit traffic sent to addresses !--
configured within the infrastructure address space. access-list transit-acl-policy
extended deny ip any 192.168.1.0 255.255.255.0 ! !-- Permit/Deny all other Layer 3
and Layer 4 traffic in accordance with !-- existing security policies and
configurations. ! !-- Apply tACL to interface(s) in the ingress direction. access-
group transit-acl-policy in interface outside !
```

Identificazione: Access Control List transit

Con un ACL, dopo aver applicato l'elenco degli accessi a un'interfaccia nella direzione in entrata, il comando **show access-list** può essere usato per identificare il numero di pacchetti HTTP e HTTPS sulle porte TCP 80 e 443 che vengono filtrati. I pacchetti filtrati devono essere esaminati per determinare se sono tentativi di sfruttare questa vulnerabilità. Di seguito è riportato un esempio di output per **show access-list-transit-acl-policy**:

```
firewall# show access-list transit-acl-policy
access-list transit-acl-policy line 1 extended deny tcp any 192.168.1.0 255.255.255.0
eq www (hitcnt=11)
access-list transit-acl-policy line 2 extended deny tcp any 192.168.1.0 255.255.255.0
eq https (hitcnt=6)
access-list transit-acl-policy line 3 extended deny ip any 192.168.1.0 255.255.255.0
(hitcnt=0)

-- Transit ACL Policy Truncated --
firewall#
```

Nell'esempio precedente, l'elenco degli accessi *transit-acl-policy* ha scartato 11 pacchetti HTTP destinati alla porta TCP 80 e sei pacchetti HTTPS destinati alla porta TCP 443 ricevuti da host o reti non attendibili. Questo ACL viene applicato all'interfaccia *esterna* in direzione in entrata.

Identificazione: Messaggi syslog firewall

Il messaggio syslog del firewall 106023 verrà generato per i pacchetti negati da una voce ACE che non ha la parola chiave **log** presente. Per ulteriori informazioni su questo messaggio syslog, consultare il documento Cisco Security Appliance System Log Message - 106023.

Per informazioni sulla configurazione del syslog per Cisco ASA serie 5500 Adaptive Security Appliance o Cisco PIX serie 500 Security Appliance, consultare il documento sulla configurazione della registrazione su Cisco Security Appliance. 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 sulla configurazione della registrazione su Cisco Security Appliance.

Negli esempi seguenti, il comando **show logging | il** comando **grep regex** viene usato per estrarre i messaggi syslog dal buffer di registrazione sul firewall. Questa operazione viene effettuata per ottenere informazioni aggiuntive sui pacchetti rifiutati che potrebbero indicare potenziali tentativi di sfruttare la vulnerabilità descritta in questo documento. È possibile utilizzare diversi modelli regex con la parola chiave **grep** per cercare dati specifici presenti all'interno dei messaggi registrati. In alcuni casi, è possibile identificare più rapidamente il traffico dannoso utilizzando più comandi **grep** ed espressioni regolari.

```
firewall#show logging | grep 106023
Apr 11 2007 14:31:17: %ASA-4-106023: Deny tcp src outside:192.168.208.63/34938 dst
inside:192.168.1.5/80 by access-group "transit-acl-policy" [0x55c1c7ff, 0x0]
Apr 11 2007 14:31:18: %ASA-4-106023: Deny tcp src outside:192.168.208.63/34939 dst
inside:192.168.1.5/80 by access-group "transit-acl-policy" [0x55c1c7ff, 0x0]
Apr 11 2007 14:31:25: %ASA-4-106023: Deny tcp src outside:192.168.208.63/34940 dst
inside:192.168.1.6/80 by access-group "transit-acl-policy" [0x55c1c7ff, 0x0]
```

Nell'esempio precedente, i messaggi (106023) registrati per il tACL *transit-acl-policy* mostrano i pacchetti HTTP e HTTPS per le porte TCP 80 e 443 inviati al blocco di indirizzi assegnato all'infrastruttura di rete. Quando gli amministratori identificano indirizzi di origine dannosi, potrebbero voler utilizzare i comandi **grep** con gli indirizzi IP dannosi associati per verificare se ci sono stati altri tentativi. Può essere prudente ricercare i dati di registro archiviati per verificare quali altre attività sono state associate agli indirizzi IP dannosi.

Per ulteriori informazioni sui messaggi syslog per appliance di sicurezza ASA e PIX, consultare il documento Cisco Security Appliance System Log Messages (Messaggi del registro di sistema di Cisco Security Appliance). Per ulteriori informazioni sui messaggi syslog per il modulo FWSM, consultare i messaggi di registrazione relativi alla configurazione dello switch Catalyst serie 6500 e del modulo servizi firewall del router Cisco serie 7600 e al log di sistema.

Ulteriori informazioni

Cronologia delle revisioni

Revisione 1.0	25 aprile 2007	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

- Protezione del core: Access Control List di protezione dell'infrastruttura
- Access Control List transit: filtraggio sul perimetro della rete
- Cisco IOS NetFlow - Home Page su Cisco.com
- White paper su Cisco IOS NetFlow
- White paper su Cisco Network Foundation Protection
- Presentazioni di Cisco Network Foundation Protection
- Prodotti Cisco Firewall - Home Page su Cisco.com

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).