여러 웹 기반 관리 인터페이스에서 PHP HTML 엔티티 인코더 힙 오버플로 취약성 식별 및 완화

여러 웹 기반 관리 인터페이스에서 PHP HTML 엔티티 인코더 힙 오버플로 취약성 식별 및 완화

권고 사항 ID: cisco-amb-20070425-http

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

개정 1.0

2007년 4월 25일 16:00 UTC(GMT) 공개 릴리스의 경우

목차

Cisco의 대응

이 Applied Mitigation Bulletin은 PSIRT Security Response: PHP HTML Entity Encoder Heap Overflow Vulnerability in Multiple Web-Based Management Interfaces(PSIRT 보안 응답의 PHP HTML 엔티티 인코더 힙 오버플로 취약성에 대한 추가 문서입니다. 네트워크 내 Cisco 디바이스에 구축할 수 있는 추가 완화 기술을 문서화합니다.

취약성 특성

특정 Cisco 제품에 포함된 특정 PHP 함수에는 취약성이 존재합니다. 인증된 공격자는 이 취약성을 원격으로 악용할 수 있습니다. 사용자 상호 작용이 필요하지 않습니다. 이 취약성을 성공적으로 악용하면 권한이 없는 코드를 실행할 수 있습니다. 이 취약성을 악용하는 데 사용되는 벡터는 HTTP 및 HTTPS 프로토콜(TCP 포트 80 및 443)입니다. 이 취약성은 CVE ID 2006-5465에서 다룹니다.

취약한, 영향을 받지 않는, 그리고 고정된 소프트웨어에 대한 정보는 PSIRT Security Response(PSIRT 보안 응답)(https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070425-http)에서 확인할 수 있습니다.

완화 기법 개요

Cisco 디바이스는 PHP HTML 엔티티 인코더 힙 오버플로 취약성에 대한 몇 가지 대응책을 제공합니다. 이러한 보호 방법 중 상당수는 인프라 디바이스 및 네트워크를 통과하는 트래픽에 대한 일반적인 보안 모범 사례로 간주되어야 합니다.

Cisco IOS Software는 iACL(infrastructure access control list)을 사용하여 효과적인 익스플로잇 방지 수단을 제공할 수 있습니다. Cisco ASA, PIX 및 FWSM(Firewall Services Module) 방화벽은 tACL(transit access control list)을 사용하여 효과적인 익스플로잇 방지 수단을 제공할 수도 있습니다. 인프라 및 트랜짓 ACL(Access Control List)은 모두 이 문서에 설명된 취약성을 악용하려는 패킷의 소스 IP 주소를 필터링 및 삭제(폐기)합니다.

탐정 제어는 Cisco IOS NetFlow에서 플로우 레코드를 사용하고 Cisco IOS Software, Cisco ASA 5500 Series Adaptive Security Appliance, Cisco PIX 500 Series Security Appliance, Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터용 FWSM에서 syslog 메시지 및 **show** 명령 출력에 표시되는 카운터 값을 통해 수행할 수 있습니다.

위험 관리

조직은 표준 위험 완화 프로세스에 따라 이 취약성의 잠재적 영향을 판단해야 합니다. 위험 분류에 도움이 될 수 있는 문서는 보안 취약성 공지 및 위험 분류와 프로토타이핑에 대한 위험 분류에서 제공됩니다.

디바이스별 완화 및 식별

주의: 어떤 완화 기술이든 효과는 제품 혼합, 네트워크 토폴로지, 트래픽 동작, 조직 임무 등 특정 고객 상황에 따라 달라집니다. 모든 컨피그레이션 변경과 마찬가지로, 변경 사항을 적용하기 전에 이 컨피그레이션의 영향을 평가합니다.

완화 및 식별에 대한 구체적인 정보는 다음 디바이스에 제공됩니다.

- Cisco IOS 라우터
- Cisco IOS NetFlow
- Cisco ASA, PIX 및 FWSM 방화벽

Cisco IOS 라우터

완화: 인프라 액세스 제어 목록

인프라 디바이스를 보호하고 직접 인프라 공격의 위험, 영향 및 효과를 최소화하기 위해 인프라 액세스 제어 목록 iACL을 구축하여 인프라 장비에 전송된 트래픽의 정책 시행을 수행해야 합니다. 관리자는 기존 보안 정책 및 컨피그레이션에 따라 인프라 디바이스로 전송되는 승인된 트래픽만 명시적으로 허용하여 iACL을 구성할 수 있습니다. 인프라 디바이스를 최대한 보호하려면 계층 3 IP 주소가 구성된 모든 인터페이스에 인그레스 방향으로 iACL을 적용해야 합니다.

다음 예에서 주소 블록 192.168.1.0/24은 인프라 주소 공간입니다. iACL 정책은 TCP 포트 80 및 443을 대상으로 하며 인프라 주소 공간의 일부인 주소로 전송되는 HTTP 및 HTTPS 패킷을 거부합니다. 인프라 디바이스로 직접 전송되는 모든 트래픽을 거부하기 전에 라우팅 및 관리 액세스에 필요한 트래픽을 허용하도록 주의해야 합니다. 인프라 주소 공간은 가능한 경우 사용자 및 서비스 세그먼트에 사용되는 주소 공간과 구분되어야 합니다. 이 주소 지정 방법론을 사용하면 iACL의 구축 및 구축에 도움이 됩니다.

추가된 ACE(Access Control Entry)는 네트워크 인그레스 포인트에서 트래픽을 필터링하는 데 사용되는 iACL 정책의 일부로 구현해야 합니다.

iACL에 대한 추가 정보는 Protecting Your Core: Infrastructure Protection Access Control Lists(코어 보호: 인프라 보호 액세스 제어 목록)에서 확인할 수 있습니다.

```
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 !
```

인터페이스 액세스 목록으로 필터링하면 ICMP 도달 불가 메시지를 필터링된 트래픽의 소스로 다시 전송합니다. 필터링 디바이스가 이러한 ICMP 도달 불가 메시지를 생성해야 하기 때문에 CPU 사용률이 증가하는 원치 않는 결과가 발생할 수 있습니다. IOS에서 ICMP 연결 불가능 생성은 500밀리초마다 하나의 패킷으로 제한됩니다. ICMP 연결 불가능 메시지 생성은 **no icmp unreachable** interface configuration 명령을 사용하여 비활성화할 수 **있습니다**. ICMP 연결 불가 속도 제한은 글로벌 컨피그레이션 명령 **ip icmp rate-limit unreachable** *interval-in-ms*를 사용하여 500밀리초당 기본값에서 변경할 수 있습니다. 관리자는 1~4294967295밀리초 사이의 간격을 지정할 수 있습니다.

식별: 인프라 액세스 제어 목록

iACL에서는 액세스 목록이 인그레스 방향의 인터페이스에 적용되면 **show access-list 명령**을 사용하여 필터링되는 TCP 포트 80 및 443의 HTTP 및 HTTPS 패킷 수를 식별할 수 있습니다. 필터링된 패킷을 조사하여 이 취약성을 악용하려는 시도인지 확인해야 합니다. show access-**list infrastructure-acl-policy의 출력** 예는 다음과 같습니다.

```
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#
```

앞의 예에서 액세스 목록 *infrastructure-acl-policy*는 ACE 시퀀스 ID 10의 경우 TCP 포트 80에서 92개의 HTTP 패킷을, ACE 시퀀스 ID 20의 경우 TCP 포트 443에서 23개의 HTTPS 패킷을 삭제했습니다. 이 iACL은 인그레스 방향으로 인터페이스 GigabitEthernet0/0에 적용됩니다.

Cisco IOS NetFlow

식별: NetFlow 레코드를 사용한 트래픽 흐름 식별

Cisco IOS 라우터 및 스위치에서 Cisco IOS NetFlow를 구성하여 이 문서에 설명된 취약성을 악용하려는 잠재적 시도일 수 있는 트래픽 흐름을 식별할 수 있습니다. 패킷이 이 취약성을 악용하려는 시도인지 또는 합법적인 트래픽인지 여부를 조사해야 합니다.

```
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
```

앞의 예에서는 포트 443의 HTTPS 프로토콜에 대해 여러 플로우가 있습니다(16진수 값 <01BB>). 이 트래픽은 10.21.96.74에서 소싱되고 192.168.1.11로 전송되며, 이는 인프라 디바이스에 사용됩니다. 네트워크 관리자는 include 문을 사용하여 특정 대상 IP 주소 또는 대상 포트만 포함시킴으로써 NetFlow 출력이 더 연관성이 높은 데이터로 제한할 수 있습니다. 예를 들면 show ip cache

flow가 있습니다 |에는 TCP 포트 443(16진수 값 <01BB>)이 사용 중인 호스트만 표시하는 01BB가 포함됩니다. 이러한 플로우를 조사하여 플로우가 신뢰할 수 없는 호스트 및/또는 네트워크에서 소싱되는지 확인해야 합니다.

Cisco ASA, PIX 및 FWSM 방화벽

완화: 통과 액세스 제어 목록

인그레스 액세스 포인트에서 네트워크로 들어오는 에지 트래픽 또는 네트워크를 전송하는 트래픽으로부터 네트워크를 보호하기 위해 이 트래픽에 대한 정책 시행을 수행하려면 tACL(transit access control list)을 구축해야 합니다. 관리자는 승인 받은 트래픽만 인그레스 액세스 포인트에서 네트워크에 들어가도록 명시적으로 허용하거나 기존 보안 정책 및 컨피그레이션에 따라 인증 받은 트래픽이 네트워크를 통과하도록 허용하여 tACL을 구성할 수 있습니다.

다음 예에서 주소 블록 192.168.1.0/24은 인프라 주소 공간입니다. tACL 정책은 인프라 주소 공간의 일부인 주소로 전송된 TCP 포트 80(HTTP) 및 443(HTTPS)에서 인증되지 않은 패킷을 거부합니다

모든 무단 트래픽을 거부하기 전에 라우팅 및 관리 액세스에 필요한 트래픽을 허용하도록 주의해야 합니다. 인프라 주소 공간은 가능한 경우 사용자 및 서비스 세그먼트에 사용되는 주소 공간과 구분되어야 합니다. 이 주소 지정 방법론을 사용하면 tACL의 구축 및 구축에 도움이 됩니다.

tACL에 대한 추가 정보는 Transit Access Control Lists: Filtering at Your Edge에서 확인할 수 있습니다.

```
!-- 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 !
```

식별: 통과 액세스 제어 목록

tACL에서는 액세스 목록이 인그레스 방향의 인터페이스에 적용되면 **show access-list 명령**을 사용하여 필터링되는 TCP 포트 80 및 443의 HTTP 및 HTTPS 패킷 수를 식별할 수 있습니다. 필터링된 패킷을 조사하여 이 취약성을 악용하려는 시도인지 확인해야 합니다. **show access-list transit-acl-policy**의 출력 **예는 다음과** 같습니다.

```
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#
```

앞의 예에서 액세스 목록 *transit-acl-policy*는 TCP 포트 80을 대상으로 하는 HTTP 패킷 11개와 신뢰할 수 없는 호스트 또는 네트워크로부터 수신한 TCP 포트 443을 대상으로 하는 HTTPS 패킷 6개를 삭제했습니다. 이 tACL은 인그레스 방향의 *외부* 인터페이스에 적용됩니다.

식별: 방화벽 Syslog 메시지

log 키워드가 106023 ACE에 의해 거부된 패킷에 대해 방화벽 syslog 메시지 **메시지**가 생성됩니다. 이 syslog 메시지에 대한 추가 정보는 Cisco Security Appliance System Log Message - 106023에서 확인할 수 있습니다.

Cisco ASA 5500 Series Adaptive Security Appliance 또는 Cisco PIX 500 Series Security Appliance에 대한 syslog 구성 정보는 Cisco Security Appliance에서 로깅 구성을 참조하십시오. Cisco Catalyst 6500 Series 스위치 및 Cisco 7600 Series 라우터에 대한 FWSM의 syslog 구성에 대한 정보는 Cisco Security Appliance의 Configuring Logging에서 확인할 수 있습니다.

다음 예에서는 **show logging | grep regex** 명령은 방화벽의 로깅 버퍼에서 syslog 메시지를 추출하는 데 사용됩니다. 이 작업은 이 문서에 설명된 취약성을 악용하려는 잠재적인 시도를 나타낼 수 있는 거부된 패킷에 대한 추가 정보를 얻기 위해 수행됩니다. logged 메시지에 있는 특정 데이터를 검색하기 위해 **grep 키워드**에 다른 regex 패턴을 사용할 수 있습니다. 경우에 따라 여러 **grep** 명령 및 정규식을 사용하여 악성 트래픽을 보다 빠르게 식별할 수 있습니다.

```
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]
```

앞의 예에서 tACL *transit-acl-policy*에 대해 로깅된 메시지(106023)는 네트워크 인프라에 할당된 주소 블록으로 전송된 TCP 포트 80 및 443에 대한 HTTP 및 HTTPS 패킷을 표시합니다. 관리자는 악의적인 소스 주소를 식별할 때 연결된 악의적인 IP 주소와 함께 **grep** 명령을 사용하여 다른 시도가 있었는지를 확인할 수 있습니다. 저장된 로그 데이터를 조사하여 악성 IP 주소와 어떤 다른 활동이 연관되었는지 확인하는 것이 신중할 수 있습니다.

ASA 및 PIX 보안 어플라이언스의 syslog 메시지에 대한 추가 정보는 Cisco Security Appliance System Log Messages에서 확인할 수 있습니다. FWSM에 대한 syslog 메시지에 대한 추가 정보는 Catalyst 6500 Series Switch 및 Cisco 7600 Series Router Firewall Services Module 로깅 컨피그레이션 및 시스템 로그 메시지에서 확인할 수 있습니다.

추가 정보

개정 이력

개정 1.0	2007년 4월 25일	초기 공개

Cisco 보안 절차

Cisco 제품의 보안 취약성 보고, 보안 사고에 대한 지원 요청, Cisco의 보안 정보 수신을 위한 등록 등에 대한 자세한 내용은 Cisco의 전 세계 웹 사이트 (https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html)에서 확인할 수 있습니다. 여기에는 Cisco 보안 알림과 관련된 언론 문의에 대한 지침이 포함됩니다. 모든 Cisco 보안 권고 사항은 http://www.cisco.com/go/psirt에서 확인할 수 있습니다.

관련 정보

- 코어 보호: 인프라 보호 액세스 제어 목록
- 트랜짓 액세스 제어 목록: 에지에서 필터링
- Cisco IOS NetFlow - 홈 페이지(Cisco.com)
- Cisco IOS NetFlow 백서
- Cisco 네트워크 기반 보호 백서
- Cisco Network Foundation Protection 프레젠테이션
- Cisco 방화벽 제품 - 홈 페이지 Cisco.com

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.