

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the PHP HTML Entity Encoder Heap Overflow Vulnerability in Multiple Web-Based Management Interfaces

Document ID: 91431

<http://www.cisco.com/warp/public/707/cisco-amb-20070425-http.shtml>

Revision 1.0

Last Updated 2007 April 25 1600 UTC (GMT)

For Public Release 2007 April 25 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

[Cisco Response](#)
[Device-Specific Mitigation and Identification](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)
[Related Information](#)

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Response: PHP HTML Entity Encoder Heap Overflow Vulnerability in Multiple Web-Based Management Interfaces. It documents additional mitigation techniques that can be deployed on Cisco devices within the network.

Vulnerability Characteristics

A vulnerability exists in certain PHP functions that are included with specific Cisco products. An authenticated attacker can exploit this vulnerability remotely. No user interaction is necessary. Successful exploitation of this vulnerability may allow unprivileged code execution. The vectors used to exploit this vulnerability are the HTTP and HTTPS protocols (TCP ports 80 and 443). This vulnerability is covered by CVE ID 2006-5465.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Response at <http://www.cisco.com/warp/public/707/cisco-sr-20070425-http.shtml>

Mitigation Technique Overview

Cisco devices provide several countermeasures for the PHP HTML entity encoder heap overflow vulnerability. Many of these protection methods should be considered general security best practices for infrastructure devices and the traffic that transits the network.

Cisco IOS Software can provide effective means of exploit prevention using infrastructure access control lists (iACLs). Cisco ASA, PIX, and Firewall Services Module (FWSM) firewalls can also provide effective means of exploit prevention using transit access control lists (tACLs). Both infrastructure and transit access control lists (ACLs) filter and drop (discard) the source IP address of packets that are trying to exploit the vulnerability described in this document.

Detective controls can be performed by Cisco IOS NetFlow using flow records and by Cisco IOS Software, Cisco ASA 5500 Series Adaptive Security Appliance, Cisco PIX 500 Series Security Appliance, and the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers through syslog messages and the counter values displayed in the output from **show** commands.

Risk Management

Organizations should follow their standard risk mitigation process to determine the potential impact of this vulnerability. Documents that may be used to aid in risk triage are available at [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#).

Device–Specific Mitigation and Identification



Caution: The effectiveness of any mitigation technique is dependent on specific customer situations

such as product mix, network topology, traffic behavior, and organizational mission. As with any configuration change, evaluate the impact of this configuration prior to applying the change.

Specific information on mitigation and identification is available for the following devices:

- [Cisco IOS Routers](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)

Cisco IOS Routers

Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, infrastructure access control lists iACLs should be deployed to perform policy enforcement of traffic sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For maximum protection of infrastructure devices, iACLs should be applied in the ingress direction to all interfaces on which a Layer 3 IP address has been configured.

In the following example, the address block 192.168.1.0/24 is the infrastructure address space. The iACL policy denies HTTP and HTTPS packets destined to TCP ports 80 and 443 and sent to addresses that are part of the infrastructure address space. Care should be taken to allow required traffic for routing and administrative access prior to denying all traffic sent directly to infrastructure devices. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

Added access control entries (ACEs) should be implemented as part of an iACL policy that is used to filter traffic at network ingress points.

Additional information about iACLs is available at [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```
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

!
```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. This could have the undesired effect of increasing CPU utilization because the filtering device needs to generate these ICMP unreachable messages. In IOS, ICMP unreachable generation is limited to one packet every 500 milliseconds. ICMP unreachable message generation can be disabled using the interface configuration command **no icmp unreachables**. ICMP unreachable rate limiting can be changed from the default of one per 500 milliseconds using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**. Administrators can specify intervals from 1 through 4294967295 milliseconds.

Identification: Infrastructure Access Control Lists

With an iACL, once the access list has been applied to an interface in the ingress direction, the **show access-list** command can be used to identify the number of HTTP and HTTPS packets on TCP ports 80 and 443 that are being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list infrastructure-acl-policy** follows:

```
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#
```

In the preceding example, the access list *infrastructure-acl-policy* has dropped 92 HTTP packets on TCP port 80 for ACE sequence ID 10 and 23 HTTPS packets on TCP port 443 for ACE sequence ID 20. This iACL is applied to the interface GigabitEthernet0/0 in the ingress direction.

Cisco IOS NetFlow

Identification: Traffic Flow Identification Using NetFlow Records

Cisco IOS NetFlow can be configured on Cisco IOS routers and switches to aid in the identification of traffic flows that may be potential attempts to exploit the vulnerability described in this document. Packets should be investigated to determine whether they are attempts to exploit this vulnerability or legitimate traffic.

```
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
```

In the preceding example, there are multiple flows for the HTTPS protocol on port 443 (hex value <01BB>). This traffic is being sourced from 10.21.96.74 and sent to address 192.168.1.11, which is used for infrastructure devices. Network administrators can use **include** statements to include only certain destination IP addresses or destination ports to restrict the NetFlow output to data that is more likely to be relevant. An example would be **show ip cache flow | include 01BB**, which would show only hosts for which TCP port 443 (hex value <01BB>) is in use. These flows should be investigated to determine whether the flows are sourced from nontrusted host(s) and/or network(s).

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

In an effort to protect the network from edge traffic that enters the network at ingress access points or traffic that transits the network, transit access control lists (tACLs) should be deployed to perform policy enforcement for this traffic. Administrators can construct a tACL by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations.

In the following example, the address block 192.168.1.0/24 is the infrastructure address space. The tACL policy denies unauthorized packets on TCP ports 80 (HTTP) and 443 (HTTPS) sent to addresses that are part of the infrastructure address space

Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of tACLs.

Additional information about tACLs is available at [Transit Access Control Lists: Filtering at Your Edge](#).

```
!-- 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

!

```

Identification: Transit Access Control Lists

With a tACL, once the access list has been applied to an interface in the ingress direction, the **show access-list** command can be used to identify the number of HTTP and HTTPS packets on TCP ports 80 and 443 that are being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. An example output for **show access-list transit-acl-policy** follows:

```

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
access-list transit-acl-policy line 2 extended deny tcp any 192.168.1.0 255.255.255.0 eq https
access-list transit-acl-policy line 3 extended deny ip any 192.168.1.0 255.255.255.0 (hit)

-- Transit ACL Policy Truncated --
firewall#

```

In the preceding example, the access list *transit-acl-policy* has dropped 11 HTTP packets destined for TCP port 80 and six HTTPS packets destined for TCP port 443 received from nontrusted hosts or networks. This tACL is applied to the interface *outside* in the ingress direction.

Identification: Firewall Syslog Messages

Firewall syslog message 106023 will be generated for packets denied by an ACE that does not have the **log** keyword present. Additional information about this syslog message is available at [Cisco Security Appliance System Log Message – 106023](#).

Information on configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is available at [Configuring Logging on the Cisco Security Appliance](#). Information on configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available at [Configuring Logging on the Cisco Security Appliance](#).

In the following examples, the **show logging | grep regex** command is used to extract syslog messages from the logging buffer on the firewall. This is performed to obtain additional information about denied packets that could indicate potential attempts to exploit the vulnerability described in this document. It is possible to use different regex patterns with the **grep** keyword to search for specific data present within the logged messages. In some cases, it is possible to more quickly identify malicious traffic by using multiple **grep** commands and regular expressions.

```

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:
Apr 11 2007 14:31:18: %ASA-4-106023: Deny tcp src outside:192.168.208.63/34939 dst inside:
Apr 11 2007 14:31:25: %ASA-4-106023: Deny tcp src outside:192.168.208.63/34940 dst inside:

```

In the preceding example, the messages (106023) logged for the tACL *transit-acl-policy* show HTTP and HTTPS packets for TCP ports 80 and 443 sent to the address block assigned to the network infrastructure. When administrators identify malicious source addresses, they may want to use **grep** commands with the associated malicious IP addresses to see if there have been other attempts. It may be prudent to research stored log data to see what other activity has been associated with the malicious IP addresses.

Additional information about syslog messages for ASA and PIX security appliances is available at [Cisco](#)

[Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is available at [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages](#).

Additional Information

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Revision History

Revision 1.0	2007 April 25	Initial public release
--------------	---------------	------------------------

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Related Information

- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Cisco IOS NetFlow – Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [Cisco Firewall Products – Home Page on Cisco.com](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Apr 25, 2007

Document ID: 91431
