

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Vulnerability in Cisco WebEx Meeting Manager ActiveX Control

<http://www.cisco.com/warp/public/707/cisco-amb-20080814-webex.shtml>

Revision 1.2

Last Updated 2008 August 18 1730 UTC (GMT)

For Public Release 2008 August 15 0130 UTC (GMT)

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

Contents

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

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory Vulnerability in Cisco WebEx Meeting Manager ActiveX Control and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

The Cisco WebEx Meeting Manager contains a buffer overflow vulnerability in an ActiveX control used by the Cisco WebEx Meeting Manager. This vulnerability can be exploited remotely without

authentication and requires end-user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution or result in a denial of service (DoS) condition. Legitimate access to the Cisco WebEx Meeting Manager is through the HTTPS protocol using TCP port 443, however an attacker could host the malicious content on any TCP port. For this particular vulnerability, mitigation will be focused on ports normally associated with HTTP traffic which include TCP ports 80, 3128, 8000, 8010, 8080, 8888, and 24326.

This vulnerability has been assigned CVE identifier CVE- 2008-3558.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/customer/707/cisco-sa-20080814-webex.shtml> .

Mitigation Technique Overview

Cisco devices provide several countermeasures for this vulnerability. Administrators are advised to consider these protection methods to be general security best practices for infrastructure devices and the traffic that transits the network. This section of the document provides an overview of these techniques.

Effective exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using application layer protocol inspection.

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit this vulnerability.

Cisco ASA appliances, Cisco PIX security appliances, and FWSM firewalls can provide visibility through syslog messages and the counter values displayed in the output from **show** commands.

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can also provide visibility through incidents, queries, and event reporting.

Risk Management

Organizations are advised to follow their standard risk evaluation and mitigation processes to determine the potential impact of this vulnerability. Triage refers to sorting projects and prioritizing efforts that are most likely to be successful. Cisco has provided documents that can help organizations develop a risk-based triage capability for their information security teams. [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#) can help organizations develop repeatable security evaluation and response processes.

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 about mitigation and identification is available for these devices:

- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco Intrusion Prevention System](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Application Layer Protocol Inspection

Application layer protocol inspection is available beginning in software release 7.2(1) for the Cisco ASA 5500 Series Adaptive Security Appliance and the Cisco PIX 500 Series Security Appliance and in software release 4.0(1) for the Firewall Services Module. This advanced security feature performs deep packet inspection of traffic that transits the firewall. Administrators may construct an inspection policy for applications that require special handling through the configuration of **inspect class-maps** and **inspect policy-maps**, which are applied via a global or interface service policy.

Additional information about application layer protocol inspection is in the [Applying Application Layer Protocol Inspection](#) section of the [Cisco Security Appliance Command Line Configuration Guide](#).

Caution: Application layer protocol inspection will decrease firewall performance. Administrators are advised to test performance impact in a lab environment before this feature is deployed in production environments.

HTTP Application Inspection

By using the HTTP inspection engine on the Cisco ASA 5500 Series Adaptive Security Appliances, the Cisco PIX 500 Series Security Appliances, and the Firewall Services Module, administrators can configure regular expressions (regexs) for pattern matching, inspection class-maps, and inspection policy-maps that can protect against specific vulnerabilities, such as the one described in this document, and other threats that may be associated with HTTP traffic. The following HTTP application inspection configuration uses the Cisco Modular Policy Framework (MPF) to create a policy for inspection of traffic on TCP ports 80, 3128, 8000, 8010, 8080, 8888, and 24326, which are the default ports for the Cisco IPS #WEBPORTS variable. The HTTP application inspection policy will drop connections where the HTTP response body contains any either of the regexs that are configured to match the ActiveX control that is associated with this vulnerability.



Caution: The configured regexs can match text strings at any location in the body of an HTML response. Care should be taken to ensure that legitimate business applications that use matching text strings without calling the ActiveX control are not affected. Additional information about regex syntax is in [Creating a Regular Expression](#).

```
!
!-- Configure regexs for the ActiveX Class ID
!-- "32E26FD9-F435-4A20-A561-35D4B987CFDC" and Program ID
!-- "WebexUCFObject.WebexUCFObject.1" that are associated
!-- with this vulnerability
!

regex CLSID_activeX "32[Ee]26[Ff][Dd]9[-][Ff]435[-]4[Aa]20[-][Aa]561[-]35[Dd]4
regex ProgID_activeX "WebexUCFObject.WebexUCFObject.1"
```

```
!  
!-- Configure a regex class to match on the regular  
!-- expressions that are configured above  
!  
class-map type regex match-any vulnerable-activeX-class  
  match regex CLSID_activeX  
  match regex ProgID_activeX  
  
!  
!-- Configure an object group for the default ports that  
!-- are used by the Cisco IPS #WEBPORTS variable, which  
!-- are TCP ports 80 (www), 3128, 8000, 8010, 8080, 8888,  
!-- and 24326  
!  
object-group service WEBPORTS tcp  
  port-object eq www  
  port-object eq 3128  
  port-object eq 8000  
  port-object eq 8010  
  port-object eq 8080  
  port-object eq 8888  
  port-object eq 24326  
  
!  
!-- Configure an access list that uses the WEBPORTS object  
!-- group, which will be used to match TCP packets that  
!-- are destined to the #WEBPORTS variable that is used  
!-- by a Cisco IPS device  
!  
access-list Webports-ACL extended permit tcp any any object-group WEBPORTS  
  
!  
!-- Configure a class that uses the above-configured  
!-- access list to match TCP packets that are destined  
!-- to the ports that are used by the Cisco IPS #WEBPORTS  
!-- variable  
!  
class-map Webports-Class  
  match access-list Webports-ACL  
  
!  
!-- Configure an HTTP application inspection policy that  
!-- looks for and drops connections that contain HTTP  
!-- protocol violations and looks for and drops connections  
!-- that contain the regexs for the affected ActiveX Class  
!-- ID or Program ID that are configured above  
!  
policy-map type inspect http http-Policy  
  parameters  
  
!  
!-- "protocol-violation" below is not required to  
!-- mitigate this vulnerability but is  
!-- included to provide more robust protection against  
!-- potential HTTP attacks. Care should be taken to ensure that
```

```

!-- legitimate applications that do not fully conform to
!-- HTTP protocol standards are not dropped by this inspection
!

    protocol-violation action drop-connection
    match response body regex class vulnerable-activeX-Class
    drop-connection log

!
!-- Add the above-configured "Webports-Class" that matches
!-- TCP packets that are destined to the default ports
!-- that are used by the Cisco IPS #WEBPORTS variable to
!-- the default policy "global_policy" and use it to
!-- inspect HTTP traffic that transits the firewall
!

policy-map global_policy
  class Webports-Class
    inspect http http-Policy

!
!-- By default, the policy "global_policy" is applied
!-- globally, which results in the inspection of
!-- traffic that enters the firewall from all interfaces
!

service-policy global_policy global

```

For additional information about the configuration and use of object groups, reference the Cisco Security Appliance Command Reference for [object-group](#).

Additional information about HTTP application inspection and the MPF is in the [HTTP Inspection Overview](#) section of the Cisco Security Appliance Command Line Configuration Guide.

Identification: Application Layer Protocol Inspection

Firewall syslog message *415007* will be generated when an HTTP message body matches a user-defined regular expression. The syslog message will identify the corresponding HTTP class and HTTP policy and indicate the action applied to the HTTP connection. Additional information about this syslog message is in [Cisco Security Appliance System Log Message - 415007](#).

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is in [Monitoring the Security Appliance - Configuring and Managing Logs](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is in [Monitoring the Firewall Services Module](#).

In the following example, the **show logging | grep** *regex* command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate attempts to exploit this vulnerability. Administrators can use different regular expressions with the **grep** keyword to search for specific data in the logged messages.

Additional information about regular expression syntax is in [Creating a Regular Expression](#)

HTTP Application Inspection

```

firewall#show logging | grep 415007
Aug 14 2008 14:35:54: %ASA-5-415007: HTTP - matched response
body regex class vulnerable-activeX-Class in policy-map
http-Policy, Body matched - Dropping connection from
outside:192.0.2.117/2329 to inside:192.168.60.65/80
Aug 14 2008 14:36:57: %ASA-5-415007: HTTP - matched response
body regex class vulnerable-activeX-Class in policy-map
http-Policy, Body matched - Dropping connection from
outside:192.0.2.150/2330 to inside:192.168.60.65/80

```

With HTTP application inspection enabled, the **show service-policy inspect protocol** command will identify the number of HTTP packets that are inspected and dropped by this feature. The following example shows output for **show service-policy inspect http**:

```

firewall# show service-policy inspect http
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Class-map: Webports-Class
Inspect: http http-Policy, packet 5025, drop 20, reset-drop 0
protocol violations
packet 0
match response body regex class vulnerable-activeX-Class
drop-connection log, packet 20

```

Cisco Intrusion Prevention System

Mitigation: Cisco IPS Signature Event Actions

Administrators can use the Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the vulnerability that is described in this document. Beginning with signature update S352 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability can be detected by signature 6988/0 (Signature Name: WebEx Meeting Manager ActiveX Overflow). Signature 6988/0 is enabled by default, triggers a High severity event, has a signature fidelity rating (SFR) of 95, and is configured with a default event action of **produce-alert**.

Signature 6988/0 is a meta signature and is composed of multiple subsignatures that all must be triggered to cause the meta signature to trigger. Each of the individual subsignatures therefore has no event action on its own and thus each is considered an Informational severity event.

Administrators can configure Cisco IPS sensors to perform an event action when an attack is detected. The configured event action performs preventive or deterrent controls to help protect against an attack that is attempting to exploit the vulnerability that is described in this document.

Cisco IPS sensors are most effective when deployed in inline protection mode combined with the use of an event action. Automatic Threat Prevention for Cisco IPS 6.x sensors that are deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit the vulnerability that is described in this document. Threat prevention is achieved through a default override that performs an event action for triggered signatures with a *riskRatingValue* greater than 90.

Cisco IPS 5.x sensors that are deployed in inline protection mode require an event action configured on a per-signature basis. Alternatively, administrators can configure an override that can perform an event action for any signatures that are triggered and are calculated as a high-risk threat. Using an event action

on sensors deployed in inline protection mode provides the most effective exploit prevention.

For additional information about the risk rating and threat rating calculation, reference [Risk Rating and Threat Rating: Simplify IPS Policy Management](#).

Identification: IPS Signature Events

Signature:6988/0 WebEx Meeting Manager ActiveX Overflow

```
IPS# show events alert | include 6988
evIdsAlert: eventId=1214370540454919078 severity=high vendor=Cisco
  originator:
    hostId: ips
    appName: sensorApp
    appInstanceId: 28725
  time: 2008/08/14 18:55:50 2008/08/14 18:55:50 UTC
  signature: description=WebEx Meeting Manager ActiveX Overflow id=6988 version
    subsigId: 0
    sigDetails: WebEx Meeting Manager ActiveX Overflow
    marsCategory: Penetrate/ClientExploit/Web
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.7.12
      port: 80
    target:
      addr: locality=OUT 192.168.2.11
      port: 2925
      os: idSource=unknown relevance=unknown type=unknown
  alertDetails: Component Signature List: 6988.1 5477.2 ;
  riskRatingValue: targetValueRating=medium 80
  threatRatingValue: 80
  interface: ge0_0
```

Cisco Security Monitoring, Analysis, and Response System

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can create incidents regarding events that are related to the vulnerability that is described in this document using IPS signature 6988/0 (Signature Name: WebEx Meeting Manager ActiveX Overflow). After the S352 dynamic signature update has been downloaded, using keyword **NR-6988/0** for IPS signature 6988/0 and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the incidents created by the IPS signature.

The following screen shot shows the values used to query for events that are created by IPS signatures that are related to this vulnerability:

Query Event Data
Click the cells below to change query criteria:

Query type: Event Raw Messages ranked by Time, 0h:10m

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY

Specify new message keywords:

Open Close

NR-6988/0	None	None	None	None	None	None	None	None	None
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

The following screen shot shows the query results for this vulnerability that are created by the Cisco Security MARS appliance:

CISCO

Summary Incidents Query / Reports Rules Management Admin Help

Query Batch Query Report

Aug 15, 2008 11:48:41 AM EDT

CS-MARS Standalone: R4-MARS v4.3

Query Event Data
Click the cells below to change query criteria:

Query type: Event Raw Messages ranked by Time, 0h:10m

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-6988/0	None	ANY	ANY

Save As Report Save As Rule Submit

Query Results

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Time
6478824810	Received remote Proxy Host data in	Aug 15, 2008	R4-09342480	192.280.150.65:80 -> 10.19.180.363/80:80 TCP Received remote Proxy Host data in [54479P ID	<input type="button" value="View"/>	False Positive Tuning
6478824810	ISAKMP ID Payload	11:14:56 AM CDT		Payload: [REDACTED] Time: 1210017446, Risk Rating: 24, ULAN: 0, Port List: 55730	<input type="button" value="View"/>	

1 to 1 of 1 (25 per page)

Beginning with the 4.3.1 and 5.3.1 releases of Cisco Security MARS appliances, support for the Cisco IPS dynamic signature updates feature has been added. This feature downloads new signatures from Cisco.com or from a local web server, correctly processes, and categorizes received events that match those signatures, and includes them in inspection rules and reports. These updates provide event normalization and event group mapping, and they also enable the MARS appliance to parse new signatures from the IPS devices.



Caution: If dynamic signature updates are not configured, events that match these new signatures appear as *unknown event type* in queries and reports. Because MARS will not include these events in inspection rules, incidents may not be created for potential threats or attacks that occur within the network.

By default, this feature is enabled but requires configuration. If it is not configured, the following Cisco Security MARS rule will be triggered:

System Rule: CS-MARS IPS Signature Update Failure

When this feature is enabled and configured, administrators can determine the current signature version downloaded by MARS by selecting **Help > About** and reviewing the *IPS Signature Version* value.

Additional information about dynamic signature updates and instructions for configuring dynamic signature updates are available for the Cisco Security MARS [4.3.1](#) and [5.3.1](#) releases.

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 1.2	2008- August-22	Updated CVE identifier.
Revision 1.1	2008- August-15	Addition of the Cisco Security Monitoring, Analysis, and Response System section
Revision 1.0	2008- August-15	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

- [Cisco Security Monitoring, Analysis, and Response System](#)
 - [Cisco Applied Mitigation Bulletins](#)
 - [Cisco Guide to Harden Cisco IOS Devices](#)
 - [Cisco Security Center](#)
 - [Cisco Firewall Products - Home Page on Cisco.com](#)
 - [Cisco 6.x Intrusion Prevention System](#)
 - [Cisco IPS 6.x Signature Downloads](#)
 - [Cisco IPS Signature Search Page](#)
 - [Common Vulnerabilities and Exposures \(CVE\)](#)
-

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)