Worldwide | Log In | Account | Register
cisco Products & Services Support How to Buy Training & Events Partners

Cisco Security Advisory

Vulnerability In Crypto Library

High

Advisory ID:	cisco-sa-20070522-crypto
Published:	2007 May 22 13:00 GMT
Version2.0:	Final
CVSS Score:	Base - 7.8
Workarounds:	See below
Cisco Bug IDs:	CSCsd85587

CVE-2006-3894
CWE-399

Download CVRF

Download PDF

Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

IS RSA BSAFE Cryptographic Libraries ASN.1 Parsing Denial of Service Vulnerability

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS
- Cisco IOS XR
- Cisco PIX and ASA Security Appliances
- Cisco Firewall Service Module (FWSM)
- Cisco Unified CallManager

This vulnerability is assigned CVE ID CVE-2006-3894. It is externally coordinated and is tracked by the following external coordinators:

- JPCERT/CC - tracked as JVNVU#754281
- CPNI - tracked as NISCC-362917
- CERT/CC - tracked as VU#754281

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto.

Note: Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. The related advisory is published at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL

Affected Products

Vulnerable Products

This vulnerability affects all products that use affected versions of third party cryptographic libraries and enabled applications that are using crypto-related function. The following Cisco products are identified to be vulnerable:

- Cisco IOS
- Cisco IOS XR
- Cisco PIX and ASA Security Appliances (only 7.x releases are affected)
- Cisco Firewall Service Module (FWSM), only releases prior 3.1(6) are affected, 2.3(x) release are not affected
- Cisco Unified CallManager

The following text lists application layer protocols or features that must be enabled in order for a device to be vulnerable. It is sufficient that only one protocol or feature is enabled in order for a devices to be vulnerable. In order to be not vulnerable, all of the listed application protocols or features must be disabled.

Affected protocols in Cisco IOS

To determine the software running on a Cisco IOS product, log in to the device and issue the show version command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the Cisco IOS release name. Other Cisco devices will not have the show version command, or will give different output.

Only Cisco IOS images that contain the Crypto Feature Set are vulnerable. Customers who are not running an IOS image with crypto support are not exposed to this vulnerability.

Cisco IOS feature set naming indicates that IOS images with crypto support have 'K8' or 'K9' in the feature designator field.

The following example shows output from a device running an IOS image with crypto support:

```
Routershow version
Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(14)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 31-Mar-05 08:04 by yiyan
```

Since the feature set designator (IK9S) contains 'K9', it can be determine that this feature set contains crypto support.

Additional information about Cisco IOS release naming is available at the following link:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/ products_white_paper09186a008018305e.shtml.

You are affected by this vulnerability if you are running one of the vulnerable IOS software releases and have, at least one, of the following protocols or features enabled:

- Internet Security Association and Key Management Protocol (ISAKMP)
- In some IOS releases the Secure Socket Layer (SSL) may also be affected
- Threat Information Distribution Protocol (TIDP)
- Cisco IOS SIP Gateway Signaling Support Over TLS (SIP-TLS)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

As some other protocols may use affected crypto library the most accurate way to determine if your IOS release is vulnerable is to consult fixed IOS releases table.

Internet Security Association and Key Management Protocol (ISAKMP)

In order for an IOS device to be vulnerable, crypto map must be explicitly configured and applied to an interface. All authentication methods (i.e., pre-shared key, certificates) are affected.

To determine if your device has ISAKMP enabled, enter the command `show crypto isakmp policy`. Below is an example of a device that has ISAKMP enabled.

```
Router#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
more output
```

If your output is like in the following example then you do not have IKE enabled on your device.

```
Router#show crypto isakmp policy
ISAKMP is turned off
```

In Cisco IOS two features rely on ISAKMP - IPSec and Group Domain of Interpretation (GDOI). Presence of either of these features is detected by the previous example.

Prior to IOS version 12.3(2)T, IKE was enabled by default, with no crypto configuration needed for the IOS device to process IKE messages.

12.2SXD versions of Cisco IOS have IKE enabled by default. To ensure that IKE processing is disabled, enter the global configuration command `no crypto isakmp enable`.

As of IOS version 12.3(2)T (which includes all 12.4-based versions), crypto configuration is required to enable IKE message processing.

Secure Socket Layer (SSL)

In some Cisco IOS software releases the vulnerable library is used to process elements of SSL functionalities. SSL is used to protect several application layer protocols like Hyper Text Transfer Protocol over SSL (HTTPS).

HTTPS is not the only protocol that may use SSL but it is the most commonly known. In order to determine if your device has HTTPS configured enter the command `show running | include secure`. Below is an example of a device that has HTTPS enabled.

```
router#show running | include secure-server
ip http secure-server
```

Threat Information Distribution Protocol (TIDP)

To determine if your device has TDIP enabled, enter the command `show running-config | include parameter-map`. Below is an example of a device that has TDIP enabled.

```
router#show running | include parameter-map
parameter-map type tms TMS_PAR
```

Cisco IOS SIP Gateway Signaling Support Over TLS (SIP-TLS)

To determine if your device has SIP-TLS enabled, enter the command `show running-config | include crypto signaling`. Below is an example of a device that has SIP-TLS enabled.

```
router#show running | include crypto signaling
crypto signaling default trustpoint user1
```

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

To determine if your device has EAP-TLS enabled, enter the command `show running-config | include method`. Below is an example of a device that has EAP-TLS enabled.

```
Router#show running | include method
method tls
```

Affected protocols in Cisco IOS XR

You are affected by this vulnerability if you are running one of the vulnerable Cisco IOS XR software releases and have, at least one, of the following protocols or features enabled:

- Internet Security Association and Key Management Protocol (ISAKMP)
- In some IOS XR releases the Secure Socket Layer (SSL) may also be affected
- Secure Shell (SSH)

In the case of IOS XR, successful exploitation will not crash the whole device but only the affected service. Successful repeated exploitation of this vulnerability may lead to a sustained Denial-of-Service (DoS) of affected services but not the whole device.

Internet Security Association and Key Management Protocol (ISAKMP)

To determine if your device has ISAKMP enabled, enter the command `show running-config | include isakmp`. Below is an example of a device that has IKE enabled.

```
Router#show running-config | include isakmp
       crypto isakmp
       crypto isakmp policy 1
       crypto isakmp profile profile-a
```

Secure Socket Layer (SSL)

SSL is used to provide secure communications to the application layer protocols like Hyper Text Transfer Protocol over SSL (HTTPS) and Object Request Brokers (ORB). To determine if your device has any service enabled that uses SSL, enter one of the following commands `show running-config | include http server ssl` or `show running-config | include xml agent corba ssl`. Below is an example of a device that has both of the services enabled.

```
Router#show running-config | include http server ssl
       http server ssl

Router#show running-config | include xml agent corba ssl
       xml agent corba ssl
```

Secure Shell (SSH)

SSH is an application and a protocol that provides secure replacement for the suite of Berkeley r-tools such as rsh, rlogin and rcp. It is highly preferred over Telnet for interactive sessions. To determine if your device has SSH enabled enter the command `show running-config | include ssh server`. Below is an example of a device that has SSH enabled.

```
Router#show running-config | include ssh server
       ssh server
       ssh server rate-limit 100
```

Affected protocols in Cisco PIX and ASA Security Appliances

You are affected by this vulnerability if you are running one of the vulnerable Cisco PIX and ASA software releases and have, at least one, of the following protocols or features enabled:

- Secure Shell (SSH)
- Internet Security Association and Key Management Protocol (ISAKMP)
- Secure Socket Layer (SSL)

Secure Shell (SSH)

To determine if a device has SSH enabled, enter the command `show running` and observe the output. If it contains the line as in the following example then SSH is enabled.

```
PIX#show running
....
ssh host_IP_address host_netmask interface
....
```

Internet Security Association and Key Management Protocol (ISAKMP)

To determine if a device has ISAKMP enabled, enter the command `show running` and observe the output. If it contains the lines as in the following example then ISAKMP is enabled.

```
PIX#show running
....
crypto isakmp policy 2
 authentication rsa-sig
....
```

Secure Socket Layer (SSL)

SSL is used to protect several application layer protocols like Hyper Text Transfer Protocol over SSL (HTTPS) and Cisco Adaptive Security Device Manager (ASDM) session.

To determine if a device has SSL enabled, enter the command `show running` and observe the output. If it contains the line as in the following example then SSL is enabled.

```
PIX#show running
....
http server enable
....
```

Affected protocols in Cisco Firewall Service Module (FWSM)

You are affected by this vulnerability if you are running one of the vulnerable Cisco FWSM software releases and have the following protocols or features enabled:

- Internet Security Association and Key Management Protocol (ISAKMP)

Internet Security Association and Key Management Protocol (ISAKMP)

To determine if a device has ISAKMP enabled, enter the command `show running` and observe the output. If it contains the line as in the following example then ISAKMP is enabled.

```
PIX#show running
....
isakmp enable interface-name
....
```

Affected protocols in Cisco Unified CallManager

You are affected by this vulnerability if you are running one of the vulnerable Cisco Unified CallManager software releases and have, at least one, of the following protocols or features enabled:

- Certificate Authority Proxy Function (CAPF)
- Cisco TAPI Service Provider (Cisco Unified CallManager TSP)

Certificate Authority Proxy Function (CAPF)

CAPF is automatically installed with Cisco CallManager but is disabled by default. In order to verify if CAPF is enabled on your Unified CallManager do the following steps.

- **Step 1 -** In Cisco CallManager Administration, choose **Service Service Parameter**.
- **Step 2 -** If you are running 4.x software then do the following: from the Server drop-down list box, choose the publisher database server. If you are running 5.x software then do the following: From the Server drop-down list box, choose the first node.
- **Step 3 -** From the Service drop-down list box, choose the Cisco Certificate Authority Proxy Function service.

If you are given CAPF parameters then CAPF is running on your system.

Cisco TAPI Service Provider (Cisco Unified CallManager TSP)

In order to determine if Cisco Unified CallManager TSP is installed open Windows Control Panel (**Start Control Panel**) and click on **Add/Remove Programs**. If 'Cisco Unity-CM TSP' is listed then you have it installed on your system.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability. Specifically, the following product's features or products are known not to be affected:

- **Cisco IOS**
  - Secure Shell (SSH)
  - Secure Copy (SCP)
- **Cisco Unified Call Manager**
  - Hyper Text Transfer Protocol over SSL (HTTPS)
  - Cisco Unified CallManager is configured for Secure Survivable Remote Site Telephony (SRST)
- **MeetingPlace Express and MeetingPlace for Telepresence**
- **Cisco IP Communicator**
- **All Cisco Unified IP Phones 7900 Series**
- **CIP TN3270 Server**
- **Cisco GSS 4400 Series Global Site Selector Appliances**
- **Cisco CatOS**

The list is not exhaustive.

Details

ASN.1 is defined by ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) standards and it describes, among other things, data structures for encoding values. The vulnerability addressed by this advisory is related to the implementation of parsing certain data structures and is not a vulnerability in the standard itself.

Protocols that use ASN.1 (e.g., voice over IP, Simple Network Management Protocol and others), but do not rely on the vulnerable crypto library, are not affected. This advisory only addresses an implementation issue in a particular crypto library from a single vendor.

This vulnerability is present in the following Cisco products:

- **Cisco IOS, documented as Cisco bug ID** CSCsd85587 **(** registered **customers only)**
- **Cisco IOS XR, documented as Cisco bug ID** CSCsg41084 **(** registered **customers only)**
- **Cisco PIX and ASA Security Appliances, documented as Cisco bug ID** CSCse91999 **(** registered **customers only)**
- **Cisco Firewall Services Module (FWSM), documented as Cisco bug ID** CSCsi97695 **(** registered **customers only)**
- **Cisco Unified CallManager, documented as Cisco bug ID** CSCsg44348 **(** registered **customers only)**

Workarounds

The only way to prevent a device being susceptible to the listed vulnerabilities is to disable the affected service(s). However, if regular maintenance and operation of the device relies on these services then there is no workaround.

It is possible to mitigate these vulnerabilities by preventing unauthorized hosts to access the affected devices. Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070522-crypto

Control Plane Policing (CoPP)

Control Plane Policing: IOS software versions that support **Control Plane Policing (CoPP)** can be configured to help protect the device from attacks that target the management and control planes. CoPP is available in Cisco IOS release trains 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T.

In the CoPP example below, the ACL entries that match the exploit packets with the permit action will be discarded by the policy-map drop function, while packets that match a deny action (not shown) are not affected by the policy-map drop function.

```
!-- Include deny statements up front for any protocols/ports/IP addresses that
!-- should not be impacted by CoPP
!-- Include permit statements for the protocols/ports that will be governed by CoPP
!-- port 443 - HTTPS
access-list 100 permit tcp any any eq 443
!-- port 500 - IKE
access-list 100 permit udp any any eq 500
!-- port 848 - GDOI
access-list 100 permit tcp any any eq 848
!-- port 5060 - SIP-TLS
access-list 100 permit tcp any any eq 5060
!-- port 5354 - TIDP
access-list 100 permit tcp any any eq 5354

!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices.
!
!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature.
!
class-map match-all Drop-Known-Undesirable
 match access-group 100

!
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
!
policy-map CoPP-Input-Policy
 class Drop-Known-Undesirable
  drop

!-- Apply the Policy-Map to the Control-Plane of the
!-- device.
!
control-plane
 service-policy input CoPP-Input-Policy
```

Please note that in the 12.0S, 12.2S, and 12.2SX Cisco IOS trains, the policy-map syntax is different:

```
policy-map CoPP-Input-Policy
 class Drop-Known-Undesirable
 police 32000 1500 1500 conform-action drop exceed-action drop
```

NOTE: In the above CoPP example, the ACL entries with the "permit" action that match the exploit packets result in the discarding of those packets by the policy-map drop function, while packets that match the "deny" action are not affected by the policy-map drop function.

Additional information on the configuration and use of the CoPP feature can be found at http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html and http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html .

Access Control List (ACL)

Access control lists can be used to help mitigate attacks that may try to exploit these vulnerabilities. This is done in a way that only packets from the legitimate sources are allowed to reach the device and all others are dropped.

```
access-list 101 permit tcp host legitimate_host_IP_address host router_IP_address eq 443
access-list 101 permit udp host legitimate_host_IP_address host router_IP_address eq 500
access-list 101 permit tcp host legitimate_host_IP_address host router_IP_address eq 506
access-list 101 permit tcp host legitimate_host_IP_address host router_IP_address eq 4848
access-list 101 permit tcp host legitimate_host_IP_address host router_IP_address eq 5060
access-list 101 permit tcp host legitimate_host_IP_address host router_IP_address eq 5354
access-list 101 deny tcp any any eq 443
access-list 101 deny udp any any eq 500
access-list 101 deny tcp any any eq 506
access-list 101 deny udp any any eq 4848
access-list 101 deny tcp any any eq 5060
access-list 101 deny tcp any any eq 5354
```

Fixed Software

When considering software upgrades, also consult http://www.cisco.com/go/psirt and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) describes a release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL: http://www.cisco.com/web/about/security/intelligence/ios-ref.html

Cisco IOS

Fixed Cisco IOS software releases are listed in the table below.

Major Release	**Availability of Repaired Releases**	
Affected 12.0-Based Release	**Rebuild**	**Maintenance**
12.0	No 12.0 Releases Vulnerable	
Affected 12.1-Based Release	**Rebuild**	**Maintenance**
12.1	No 12.1 Releases Vulnerable	
Affected 12.2-Based Release	**Rebuild**	**Maintenance**
12.2B	Vulnerable; migrate to 12.4(10) or later	
12.2BC	Vulnerale; migrate to 12.3(17b)BC6 or later	
12.2BZ	Vulnerable; contact TAC	
12.2CX	Vulnerale; migrate to 12.3(17b)BC6 or later	
12.2CY	Vulnerale; migrate to 12.3(17b)BC6 or later	
12.2CZ	Vulnerable; contact TAC	
12.2EWA	12.2(25)EWA9	
12.2EX	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2EY	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2EZ	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2FX	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2FY	Vulnerable; migrate to 12.2(35)SE2 or later	
12.2FZ	Vulnerable; migrate to 12.2(35)SE2 or later	
12.2JA	Vulnerable; contact TAC	
12.2JK	Vulnerable; migrate to 12.4(6)T7 or later	
12.2SB	12.2(31)SB2	
12.2SE	12.2(35)SE2	
12.2SEA	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2SEB	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2SEC	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2SED	Vulnerable; migrate to 12.2(25)SEE3 or later	
12.2SEE	12.2(25)SEE3	
12.2SEF	Vulnerable; migrate to 12.2(35)SE2 or later	
12.2SEG	Vulnerable; migrate to 12.2(35)SE2 or later	

12.2SG		12.2(37)SG
12.2SGA	12.2(31)SGA1	
12.2SRA	12.2(33)SRA3	
12.2SRB		12.2(33)SRB
12.2SXD	Vulnerable; migrate to 12.2(18)SXF8 or later	
12.2SXE	Vulnerable; migrate to 12.2(18)SXF8 or later	
12.2SXF	12.2(18)SXF8	
12.2T	Vulnerable; migrate to 12.3(22) or later	
12.2XR	Vulnerable; migrate to 12.3(22) or later	
12.2YU	Vulnerable; migrate to 12.4(10) or later	
12.2YV	Vulnerable; migrate to 12.4(10) or later	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; migrate to 12.3(22) or later	
12.2ZF	Vulnerable; migrate to 12.4(10) or later	
12.2ZG	Vulnerable; contact TAC	
12.2ZH	Vulnerable; contact TAC	
12.2ZJ	Vulnerable; migrate to 12.4(10) or later	
12.2ZL	Vulnerable; contact TAC	
12.2ZN	Vulnerable; migrate to 12.3(22) or later	
12.2ZU	Vulnerable; contact TAC	
12.2ZW	Vulnerable; contact TAC	
Affected 12.3-Based Release	**Rebuild**	**Maintenance**
12.3		12.3(22)
12.3B	Vulnerable; migrate to 12.4(10) or later	
12.3BC	12.3(17b)BC6	
	12.3(21a)BC1	
12.3JA	Vulnerable; contact TAC	
12.3JEA	Vulnerable; contact TAC	
12.3JK	Vulnerable; contact TAC	
12.3JL	Vulnerable; contact TAC	
12.3JX	Vulnerable; contact TAC	
12.3T	Vulnerable; migrate to 12.4(10) or later	
12.3TPC	Vulnerable; contact TAC	
12.3XA	Vulnerable; contact TAC	
12.3XB	Vulnerable; migrate to 12.4(10) or later	
12.3XC	Vulnerable; contact TAC	
12.3XD	Vulnerable; migrate to 12.4(10) or later	
12.3XE	Vulnerable; contact TAC	
12.3XF	Vulnerable; migrate to 12.4(10) or later	
12.3XG	Vulnerable; contact TAC	

12.3XH	Vulnerable; migrate to 12.4(10) or later	
12.3XI	Vulnerable; contact TAC	
12.3XJ	Vulnerable; contact TAC	
12.3XK	Vulnerable; migrate to 12.4(10) or later	
12.3XQ	Vulnerable; migrate to 12.4(10) or later	
12.3XR	Vulnerable; contact TAC	
12.3XS	Vulnerable; migrate to 12.4(10) or later	
12.3XU	Vulnerable; migrate to 12.4(6)T7 or later	
12.3XW	Vulnerable; contact TAC	
12.3XX	12.3(8)XX2d	
12.3YA	Vulnerable; contact TAC	
12.3YD	Vulnerable; migrate to 12.4(6)T7 or later	
12.3YF	Vulnerable; contact TAC	
12.3YG	Vulnerable; migrate to 12.4(6)T7 or later	
12.3YH	Vulnerable; migrate to 12.4(6)T7 or later	
12.3YI	Vulnerable; migrate to 12.4(6)T7 or later	
12.3YK	Vulnerable; migrate to 12.4(6)T7 or later	
12.3YQ	Vulnerable; migrate to 12.4(6)T7 or later	
12.3YS	Vulnerable; migrate to 12.4(6)T7 or later	
12.3YT	Vulnerable; migrate to 12.4(6)T7 or later	
12.3YU	Vulnerable; contact TAC	
12.3YX	12.3(14)YX7	
12.3YZ	Vulnerable; contact TAC	
Affected 12.4-Based Release	**Rebuild**	**Maintenance**
12.4	12.4(7d)	12.4(10)
12.4SW	12.4(11)SW1	
12.4T	12.4(6)T7	
	12.4(9)T3	
	12.4(11)T1	
12.4XA	Vulnerable; migrate to 12.4(6)T7 or later	
12.4XB	Vulnerable; contact TAC	
12.4XC	12.4(4)XC6	
12.4XD	12.4(4)XD6	
12.4XE	Vulnerable; contact TAC	
12.4XJ	12.4(11)XJ2	

Cisco IOS XR

The following table lists fixed Cisco IOS XR software.

Cisco IOS XR Version	SMU ID	SMU Name
3.2.3	AA01802	hfr-k9sec-3.2.3.CSCsg41084
3.2.4	AA01801	hfr-k9sec-3.2.4.CSCsg41084
3.2.6	AA01800	hfr-k9sec-3.2.6.CSCsg41084

3.3.0	AA01799, AA01780	hfr-k9sec-3.3.0.CSCsg41084
3.3.0	AA01780	c12k-k9sec-3.3.0.CSCsg41084
3.3.1	AA01781	c12k-k9sec-3.3.1.CSCsg41084
3.3.1	AA01798	hfr-k9sec-3.3.1.CSCsg41084
3.3.2	AA01797	hfr-k9sec-3.3.2.CSCsg41084
3.3.3	AA01796	hfr-k9sec-3.3.3.CSCsg41084
3.3.3	AA01785	c12k-k9sec-3.3.3.CSCsg41084
3.4.0	AA01782	c12k-k9sec-3.4.0.CSCsg41084
3.4.0	AA01795	hfr-k9sec-3.4.0.CSCsg41084
3.4.1	AA01783	c12k-k9sec-3.4.1.CSCsg41084
3.4.1	AA01794	hfr-k9sec-3.4.1.CSCsg41084

IOS XR Package Installation Envelopes (PIE) can be downloaded from File Exchange at: https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=IOS-XR (registered customers only) . Installation instructions are included in the accompanying .txt files.

Cisco PIX and ASA Security Appliance

This vulnerability is fixed in the following 7.x software releases: 7.0(6.7), 7.1(2.27), 7.2(1.22), 7.2(2). All 8.x software releases do contain the fixed library and are not affected. No 6.x software releases are affected by this vulnerability.

Cisco Firewall Service Module (FWSM)

This vulnerability is fixed in the following software releases:

- 3.1(6) maintenance release, expected in 2007-June

Cisco Unified CallManager

This vulnerability is fixed in the following software releases.

- 4.0(x) releases are vulnerable but no fix will be provided. Customers are advised to upgrade to the fixed 4.1 or 4.2 software.
- 4.1(3)sr.5 expected in 2007-May-24
- 4.2(3)sr.2 expected in 2007-May
- 4.3(1)sr.1 expected 2007-Jun
- 5.0(4) - no fixed software planned, users should upgrade to 5.1(2)
- 5.1(1) - no fixed software planned, users should upgrade to 5.1(2)
- 5.1(2)

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this Advisory.

This vulnerability was discovered by Cisco during internal testing.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto

Revision History

Revision 1.4	2008-June-27	Updated Summary to remove link and verbiage.
Revision 1.3	2007-June-28	2.3(x) release of FWSM are not affected
Revision 1.2	2007-May-25	Updated fixed IOS releases, clarified ISAKMP authentication for IOS, clarified impact on IOS XR
Revision 1.1	2007-May-22	Updated information on affected FWSM protocols, fixed type on IOS release with IKE enabled by default
Revision 1.0	2007-May-22	Initial public release.

Legal Disclaimer

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.

A stand-alone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy, and may lack important information or contain factual errors. The information in this document is intended for end-users of Cisco products.

Information For
Small Business
Midsize Business
Service Provider
Executives
Industries ›
Marketplace
Contacts
Contact Cisco
Find a Reseller

News & Alerts
Newsroom
Blogs
Field Notices
Security Advisories
Technology Trends
Cloud
Internet of Things (IoT)
Mobility
Software Defined Networking (SDN)

Support
Downloads
Documentation
Communities
DevNet
Learning Network
Support Community
Video Portal ›

About Cisco
Investor Relations
Corporate Social Responsibility
Environmental Sustainability
Tomorrow Starts Here
Our People
Careers
Search Jobs
Life at Cisco
Programs
Cisco Designated VIP Program
Cisco Powered
Financing Options

Contacts | Feedback | Help | Site Map | Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks