

Cisco Security Advisory: Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability

Advisory ID: cisco-sa-20090923-ipsec

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml>

Revision 1.2

Last Updated 2009 October 19 1600 UTC (GMT)

For Public Release 2009 September 23 1600 UTC (GMT)

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

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

Summary

Cisco IOS® devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml>.

Note: The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ **Affected Products**

Cisco IOS devices that are configured for IKE and certificate based authentication are affected, if there are RSA keys present on the device.

☐ **Vulnerable Products**

IKE is enabled by default if IPsec is used. Cisco IOS devices that are configured for IKE will listen on UDP port 500, UDP port 4500 if the device is configured for NAT Traversal (NAT-T), or UDP ports 848 or 4848 if the device is configured for Group Domain of Interpretation (GDOI). The following outputs show a router that is listening on UDP port 500:

```

Router#show ip sockets
Proto      Remote      Port          Local          Port   In
Out Stat TTY OutputIF
.....
 17    --listen--          192.168.66.129    500    0
0    11    0
.....

```

Or

```

Router-#show udp
Proto      Remote      Port          Local          Port
In Out  Stat TTY OutputIF
 17          --listen--          192.0.2.1          500
0  0  1011  0
 17(v6)    --listen--          --any--            500
0  0  20011  0
Router#

```

IKE configurations that are performing certificate based authentication will display **Rivest-Shamir-Adleman Signature** as the authentication method in the output of the **show crypto isakmp policy** command. This output is shown in the following example:

```

Router#show crypto isakmp
policy

Global IKE policy
Default protection suite
      encryption algorithm:    DES - Data Encryption
Standard (56 bit keys).
      hash algorithm:          Secure Hash Standard
      authentication method:   Rivest-Shamir-Adleman
Signature
      Diffie-Hellman group:    #1 (768 bit)
      lifetime:                86400 seconds, no
volume limit

```

The **show crypto key mypubkey rsa** command can be used to check whether there are RSA keys present on the system. This output is shown in the following example:

```

Router#show crypto key mypubkey rsa
% Key pair was generated at: 06:07:49 UTC Jan 13 1996

```

```
Key name: myrouter.example.com
Usage: Signature Key
Key Data:
  005C300D 06092A86 4886F70D 01010105 00034B00
30480241 00C5E23B
  55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820
847EDAD9 DF0B4E4C
  73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221
B583D7A4 71020301 0001

% Key pair was generated at: 06:07:50 UTC Jan 13 1996
Key name: myrouter.example.com
Usage: Encryption Key
Key Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37
C4F4B0FD 9DADE748
  429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685
2F2190A0 0B43F1BD
  9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26
DBC64468 7789F76E EE21
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco 6500 Series device that is running Cisco IOS Software release 12.2(18)SXF7 with an installed image name of s72033_rp-IPSERVICESK9_WAN-M:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-
IPSERVICESK9_WAN-M), Version 12.2(18)SXF7, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright ©) 1986-2006 by cisco Systems, Inc.
```

Compiled Thu 23-Nov-06 06:42 by kellythw
<output truncated>

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link: <http://www.cisco.com/warp/public/620/1.html>.

☐ Products Confirmed Not Vulnerable

Cisco IOS XR Software is not affected by this vulnerability.

No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IKE is a key management protocol standard that is used in conjunction with the IPsec standard.

IKE is a hybrid protocol that implements the Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and SKEME are security protocols that are implemented by IKE.). More information on IKE is available at the following link:

http://www.cisco.com/en/US/docs/ios/12_1/security/configuration/guide/scdike.html

A vulnerability exists in the IKE implementation of Cisco IOS Software, if the certificate based authentication method is used. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 SAs, which may prevent new IPsec sessions from being established.

Administrators can view Phase 1 SAs that are allocated as a result of exploitation by issuing the **show crypto isakmp sa** command. The following example displays sample output for this command:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst                src                state                conn-id
slot status
```

10.48.66.77	10.48.66.6	MM_KEY_EXCH	1004
ACTIVE			
10.48.66.77	10.48.66.6	MM_KEY_EXCH	1003
ACTIVE			
10.48.66.77	10.48.66.6	MM_KEY_EXCH	1002
ACTIVE			
....			

Any allocated SA can be de-allocated up manually by using the **clear crypto isakmp** <conn-ID> command.

This vulnerability is addressed by the Cisco Bug IDs [CSCsy07555](#) ([registered](#) customers only) and [CSCee72997](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-2868.

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsy07555 - P1 SA stuck in KEY_EXCH forever

Calculate the environmental score of [CSCsy07555](#)

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

CSCee72997 - P1 SA stuck in KEY_EXCH forever

Calculate the environmental score of [CSCee72997](#)

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 SAs, which may prevent new IPsec sessions from being established.

[Top of the section](#) [Close Section](#)

☐ Software Versions and Fixes

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) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. 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. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases		
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases		
Affected 12.2-Based Releases	First Fixed Release	Recommended Release

12.2	Not Vulnerable	
12.2B	Not Vulnerable	
12.2BC	Not Vulnerable	
12.2BW	Not Vulnerable	
12.2BX	Not Vulnerable	
12.2BY	Not Vulnerable	
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Not Vulnerable	
12.2DA	Not Vulnerable	
12.2DD	Not Vulnerable	
12.2DX	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	

12.2EX	Releases prior to 12.2(44)EX are vulnerable, release 12.2(44)EX and later are not vulnerable; migrate to any release in 12.2SEG	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2EY	Not Vulnerable	
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Not Vulnerable	
12.2IRA	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3
12.2IRB	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3
12.2IRC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXA	Not Vulnerable	
12.2IXB	Not Vulnerable	

12.2IXC	Not Vulnerable	
12.2IXD	Not Vulnerable	
12.2IXE	Not Vulnerable	
12.2IXF	Not Vulnerable	
12.2IXG	Not Vulnerable	
12.2IXH	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	
12.2S	Not Vulnerable	
12.2SB	12.2(33)SB6	12.2(31)SB16 12.2(33)SB7
12.2SBC	Not Vulnerable	
12.2SCA	Vulnerable; first fixed in 12.2SCB	12.2(33)SCB4
12.2SCB	12.2(33)SCB4	12.2(33)SCB4

12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13- OCT-2009	12.2(50)SE3 12.2(52)SE; Available on 13-OCT- 2009
12.2SEA	Not Vulnerable	
12.2SEB	Not Vulnerable	
12.2SEC	Not Vulnerable	
12.2SED	Not Vulnerable	
12.2SEE	Not Vulnerable	
12.2SEF	Not Vulnerable	
12.2SEG	Not Vulnerable	
12.2SG	Not Vulnerable	
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SQ	Not Vulnerable	
12.2SRA	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3

12.2SRB	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3
12.2SRC	12.2(33)SRC5; Available on 29-OCT-2009	12.2(33)SRD3
12.2SRD	12.2(33)SRD3 12.2(33)SRD2a	12.2(33)SRD3
12.2STE	Not Vulnerable	
12.2SU	Not Vulnerable	
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SVE	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Not Vulnerable	
12.2SXA	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Not Vulnerable	

12.2SXE	Not Vulnerable	
12.2SXF	Not Vulnerable	
12.2SXH	12.2(33)SXH6; Available on 30-OCT-2009 Please see IOS Software Modularity Patch	12.2(33)SXH6; Available on 30-OCT-2009
12.2SXI	12.2(33)SXI2a	12.2(33)SXI2a
12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Not Vulnerable	
12.2TPC	Not Vulnerable	
12.2XA	Not Vulnerable	
12.2XB	Not Vulnerable	
12.2XC	Not Vulnerable	
12.2XD	Not Vulnerable	
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	

12.2XG	Not Vulnerable	
12.2XH	Not Vulnerable	
12.2XI	Not Vulnerable	
12.2XJ	Not Vulnerable	
12.2XK	Not Vulnerable	
12.2XL	Not Vulnerable	
12.2XM	Not Vulnerable	
12.2XNA	Please see Cisco IOS-XE Software Availability	
12.2XNB	Please see Cisco IOS-XE Software Availability	
12.2XNC	Please see Cisco IOS-XE Software Availability	
12.2XND	Please see Cisco IOS-XE Software Availability	
12.2XO	Not Vulnerable	

12.2XQ	Not Vulnerable	
12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	
12.2XT	Not Vulnerable	
12.2XU	Not Vulnerable	
12.2XV	Not Vulnerable	
12.2XW	Not Vulnerable	
12.2YA	Not Vulnerable	
12.2YB	Not Vulnerable	
12.2YC	Not Vulnerable	
12.2YD	Not Vulnerable	
12.2YE	Not Vulnerable	
12.2YF	Not Vulnerable	
12.2YG	Not Vulnerable	
12.2YH	Not Vulnerable	
12.2YJ	Not Vulnerable	

12.2YK	Not Vulnerable	
12.2YL	Not Vulnerable	
12.2YM	Not Vulnerable	
12.2YN	Not Vulnerable	
12.2YO	Not Vulnerable	
12.2YP	Not Vulnerable	
12.2YQ	Not Vulnerable	
12.2YR	Not Vulnerable	
12.2YS	Not Vulnerable	
12.2YT	Not Vulnerable	
12.2YU	Not Vulnerable	
12.2YV	Not Vulnerable	
12.2YW	Not Vulnerable	
12.2YX	Not Vulnerable	
12.2YY	Not Vulnerable	
12.2YZ	Not Vulnerable	

12.2ZA	Not Vulnerable	
12.2ZB	Not Vulnerable	
12.2ZC	Not Vulnerable	
12.2ZD	Not Vulnerable	
12.2ZE	Not Vulnerable	
12.2ZF	Not Vulnerable	
12.2ZG	Not Vulnerable	
12.2ZH	Not Vulnerable	
12.2ZJ	Not Vulnerable	
12.2ZL	Not Vulnerable	
12.2ZP	Not Vulnerable	
12.2ZU	Not Vulnerable	
12.2ZX	Not Vulnerable	
12.2ZY	Not Vulnerable	
12.2ZYA	Not Vulnerable	

Affected 12.3-Based Releases	First Fixed Release	Recommended Release
12.3	Not Vulnerable	
12.3B	Not Vulnerable	
12.3BC	Not Vulnerable	
12.3BW	Not Vulnerable	
12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JEC	Not Vulnerable	
12.3JK	Not Vulnerable	
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	

12.3T	Vulnerable; first fixed in 12.4 Releases up to and including 12.3(8)T11 are not vulnerable.	12.4(25b) 12.4(23b)
12.3TPC	Not Vulnerable	
12.3VA	Not Vulnerable	
12.3XA	Not Vulnerable	
12.3XB	Not Vulnerable	
12.3XC	Not Vulnerable	
12.3XD	Not Vulnerable	
12.3XE	Not Vulnerable	
12.3XF	Not Vulnerable	
12.3XG	Not Vulnerable	
12.3XI	Not Vulnerable	
12.3XJ	Not Vulnerable	
12.3XK	Not Vulnerable	

12.3XL	Vulnerable; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3XQ	Not Vulnerable	
12.3XR	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XS	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XU	Not Vulnerable	
12.3XW	Not Vulnerable	
12.3XX	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XY	Not Vulnerable	
12.3XZ	Not Vulnerable	
12.3YA	Vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)

12.3YD	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YF	Vulnerable; migrate to any release in 12.4XN	12.4(15)XR7 12.4(22)XR
12.3YG	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YH	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YI	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.3YJ	Not Vulnerable	
12.3YK	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YM	Not Vulnerable	
12.3YQ	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YS	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.3YT	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YU	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YX	Vulnerable; migrate to any release in 12.4XN	12.4(15)XR7 12.4(22)XR
12.3YZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3ZA	Not Vulnerable	
Affected 12.4-Based Releases	First Fixed Release	Recommended Release

12.4	Releases prior to 12.4(7) are vulnerable; Releases 12.4 (7a) and later are not vulnerable.	12.4(25b) 12.4(23b)
12.4GC	Not Vulnerable	
12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JDC	Not Vulnerable	
12.4JDD	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MDA	Not Vulnerable	
12.4MR	Not Vulnerable	

12.4SW	Not Vulnerable	
12.4T	12.4(4)T8 12.4(9)T 12.4(6)T1	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XA	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XB	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XC	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.4XD	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XE	Not Vulnerable	
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Not Vulnerable	
12.4XK	Not Vulnerable	
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Not Vulnerable	

12.4XV	Not Vulnerable	
12.4XW	Not Vulnerable	
12.4XY	Not Vulnerable	
12.4XZ	Not Vulnerable	
12.4YA	Not Vulnerable	
12.4YB	Not Vulnerable	
12.4YD	Not Vulnerable	
12.4YE	Not Vulnerable	

Cisco IOS XE Software

Cisco IOS XE Software Release	First Fixed Release
2.1.x	2.3.0t
2.2.x	2.3.0t
2.3.x	Not Vulnerable
2.4.x	Not Vulnerable

Cisco IOS Software Modularity - Maintenance Packs

Customers who are using Cisco IOS Software Modularity can apply the respective maintenance packs. More information on Cisco IOS Software Modularity can be found at the following link:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd80313e15.html

The Maintenance Packs listed below can be downloaded at <http://www.cisco.com/go/pn>

Cisco IOS Software Modularity Maintenance Pack for 12.2SXH

Cisco IOS Software Release	Solution Maintenance Pack (MP)
12.2(33)SXH5	MP001

[Top of the section](#) [Close Section](#)

Workarounds

If RSA keys are not needed on the system, the **crypto key zeroize rsa** command can be used to delete all RSA keys from your system. Note that this will break all features that are using RSA keys, including the Secure Shell (SSH).

Additional mitigations that can be deployed on Cisco devices in the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory, which is available at the following link:<http://www.cisco.com/warp/public/707/cisco-amb-20090923-ipsec.shtml>

[Top of the section](#) [Close Section](#)

Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html , or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml> .

Do not contact psirt@cisco.com or security-alert@cisco.com for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **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 reported to Cisco by a customer.

[Top of the section](#) [Close Section](#)

☐ **Status of this Notice: FINAL**

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 in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.2	2009-October-19	Updated ION software table.
Revision 1.1	2009-October-02	Added crypto key zeroize rsa command as a workaround.
Revision 1.0	2009-September-23	Initial public release

[Top of the section](#) [Close Section](#)

☐ **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>.

[Top of the section](#) [Close Section](#)

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](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)