

# Cisco Security Advisory: Cisco IPSec Malformed IKE Packet Vulnerability

Advisory ID: [cisco-sa-20040408-vpnsnm](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsnm.shtml>

## Revision 2.0

Last Updated 2005 March 30 1600 UTC (GMT)

For Public Release 2004 April 8 1600 UTC (GMT)

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

## Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Versions and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of This Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

## Summary

A malformed Internet Key Exchange (IKE) packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router to reload. Only devices running Cisco IOS software with Crypto support are affected.

This vulnerability is documented as Cisco bug ID CSCed30113. There are workarounds available to mitigate the effects of this vulnerability.

Cisco has made free software available to address this vulnerability for all affected customers.

The title of this advisory has been updated from "Cisco IPSec VPN Services Module Malformed IKE Packet Vulnerability" to the current title due to a change in the products affected no longer being limited to those devices with a VPN Services Module installed.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsnm.shtml>.

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

## ▣ Affected Products

This section provides details on affected products.

### ▣ Vulnerable Products

The vulnerability is only present if a Crypto feature set is being used. Customers can verify if they are running a Crypto feature set via the **show version** command:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-PK9S-M), Version 12.2(18)SXD3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Thu 09-Dec-04 19:35 by pwade
Image text-base: 0x4002100C, data-base: 0x422E8000
```

Software that contains the 'K9' designation, as in the following line, includes the Crypto feature set:

```
IOS (tm) c6sup2_rp Software (c6sup2_rp-PK9S-M), Version 12.2(18)SXD3, RELEASE SOFTWARE (fc1)
```

All Cisco Catalyst 6500 Series Switch and the Cisco 7600 Series Internet Router hardware running the following Cisco IOS releases are affected by this vulnerability.

Release Train	Affected Releases
12.2SXA	earlier than 12.2(17b)SXA
12.2SXB	earlier than 12.2(17d)SXB
12.2SX	12.2(17a)SX through 12.2(17a)SX4
12.2SY	earlier than 12.2(14)SY3

### ▣ Products Confirmed Not Vulnerable

Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Internet Routers running Cisco IOS release train 12.1E are not affected by this vulnerability.

To determine your software revision, type **show version** at the command line prompt.

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

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

## ▣ Details

A malformed IKE packet may cause an affected device to reload.

This vulnerability could be used to conduct a Denial of Service (DoS) attack against a vulnerable device. This vulnerability is known to only exist in the modified IKE code which was incorporated in the 12.2SXA, 12.2SXB, 12.2SX and 12.2SY Cisco IOS software release trains.

Cisco IOS devices with Crypto support will process IKE messages by default. More information can be found here: [http://www.cisco.com/en/US/docs/ios/12\\_3/security/command/reference/sec\\_c2g.html](http://www.cisco.com/en/US/docs/ios/12_3/security/command/reference/sec_c2g.html)

The Internetworking Terms and Cisco Systems Acronyms online guides can be found at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/>.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID [CSCed30113](#) ( [registered](#) customers only) .

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

## ▣ Impact

Successful exploitation of this vulnerability could result in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

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

## ▣ Software Versions and Fixes

This vulnerability has been fixed in the following Cisco IOS releases for the Cisco Catalyst 6500 Series Switch and the Cisco 7600 Series Internet Router hardware:

Release Train	Fixed Releases
12.2SXA	12.2(17b)SXA and later
12.2SXB	12.2(17d)SXB and later
12.2SX	Migrate to 12.2(17d)SXB or later
12.2SY	12.2(14)SY3 and later

Please refer to these documents for more information:

- 12.2(17b)SXA Release Notes: [http://www.cisco.com/en/US/prod/collateral/routers/ps368/prod\\_bulletin09186a00801df1dd\\_ps5014\\_Products\\_Bulletin.html](http://www.cisco.com/en/US/prod/collateral/routers/ps368/prod_bulletin09186a00801df1dd_ps5014_Products_Bulletin.html)
- 12.2(17d)SXB Release Notes: [http://www.cisco.com/en/US/products/ps6017/prod\\_bulletin09186a00802078b5.html](http://www.cisco.com/en/US/products/ps6017/prod_bulletin09186a00802078b5.html)
- 12.2(14)SY3 Release Notes: [http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod\\_bulletin09186a008017dc51.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_bulletin09186a008017dc51.html)

When considering software upgrades, please also consult [http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html) 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") for assistance.

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

## Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

Customers that do not require IPSec functionality on their devices can use the command 'no crypto isakmp enable' in configuration mode to disable processing of IPSec and eliminate their exposure.

As a possible mitigation, access-lists could be applied on the affected IOS platforms to limit the source IP addresses permitted to establish IPSec sessions to the device.

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

## Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

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

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

## 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>.

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

## Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement 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.

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

## Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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](mailto:tac@cisco.com)

Have your product serial number available and give the URL of this notice as evidence of your 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](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) for additional TAC contact information, including special 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 PSIRT 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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsml.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key having the fingerprint 8C82 5207 0CA9 ED40 1DD2 EE2A 7B31 A8CF 32B6 B590 and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com
- Various internal Cisco mailing lists

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 2.0	2005-March-30	Updated the advisory to reflect devices without the VPNSM may be affected. Added 12.2(17d)SX as an affected release train. Added information for determining the presence of the crypto feature set.
Revision 1.2	2005-January-4	Updated the 12.2(14)SY03 Release Notes URL in the Software Fixes and Versions section.
Revision 1.1	2004-April-8	Removed 12.2ZA as a vulnerable Cisco IOS software release train.
Revision 1.0	2004-April-8	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](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)

Send

[Home](#) | [How to Buy](#) | [Login](#) | [Profile](#) | [Feedback](#) | [Site Map](#) | [Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)  
© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)