

# Cisco Security Advisory: Vulnerabilities in the Internet Key Exchange Xauth Implementation

Document ID: 64424

Advisory ID: cisco-sa-20050406-xauth

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

## Revision 1.0

For Public Release 2005 April 06 1600 UTC (GMT)

---

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

---

[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

Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to <http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

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

## Affected Products

This section provides details on affected products.

## Vulnerable Products

This issue affects all Cisco devices running any unfixed version of Cisco IOS that supports, and is configured for, Cisco Easy VPN Server Xauth version 6 authentication.

A Cisco device running Easy VPN Server and configured for Xauth authentication will have the following line in the configuration:

```
crypto map <mapname> client authentication list <listname>
```

The Easy VPN Server XAUTH feature may also be enabled underneath an ISAKMP profile via a configuration similar to:

```
crypto isakmp profile <profilename>
  match identity group <groupname>
  client authentication list <listname>
  isakmp authentication list <listname>
  client configuration address respond
  qos-group 2
```

To determine the software running on a Cisco 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 IOS release name. Other Cisco devices will not have the show version command or will give different output.

The following example identifies a Cisco product running IOS release 12.3(6) with an installed image name of C3640-I-M:

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-I-M), Version 12.3(6), RELEASE SOFTWARE (fc3)
```

The next example shows a product running IOS release 12.3(11)T3 with an image name of C3845-ADVIPSERVICESK9-M:

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.3(11)T3, RELEASE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

## Products Confirmed Not Vulnerable

Cisco Easy VPN Server is an IOS-only feature. Devices that do not run IOS are not vulnerable.

No other Cisco products are currently known to be affected by these vulnerabilities.

## Details

IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer allowing for data to be transmitted across a public network without fear of observation, modification, or spoofing, thus enabling applications such as Virtual Private Networks (VPNs). IPSec uses the Internet Key Exchange (IKE) protocol to provide authentication of the IPSec peers, negotiate IPSec security associations (SA), and establish IPSec keys.

Extended Authentication (XAUTH) is an extension to IKE defined in an expired Internet Engineering Task Force (IETF) Internet Draft, draft-ietf-ipsec-isakmp-xauth-06.txt, which allows for organizations to utilize existing legacy authentication methods in order to manage remote access.

Successful VPN establishment consists of two levels of SA's known as phases. Phase 1 authentication establishes session keys. Using the Xauth feature, the client waits for a "username/password" challenge after the IKE Phase 1 SA has been established. When the end user responds to the challenge, the response is forwarded to the IPsec peers for an additional level of authentication.

The [Cisco IOS Easy VPN Server feature](#) introduced in IOS 12.2(8)T allows an IOS device to act as a VPN concentrator, providing authentication and encrypted access to network resources.

To determine if Cisco's Easy VPN Server XAUTH feature is enabled, check the device's configuration for the following line:

```
crypto map <mapname> client authentication list <listname>
```

The Easy VPN Server XAUTH feature may also be enabled underneath an ISAKMP profile via a configuration similar to:

```
crypto isakmp profile <profilename>
  match identity group <groupname>
  client authentication list <listname>
  isakmp authentication list <listname>
  client configuration address respond
  qos-group 2
```

Certain packets sent to the IOS Easy VPN Server listening on User Datagram Protocol (UDP) port 500 may permit an unauthorized user to complete Xauth authentication and thereby gain access to network resources.

In order for the attack to succeed, an attacker must know the shared group key to complete the IKE Phase 1 negotiation before the Xauth negotiation takes place.

This malformed packet vulnerability is documented as Cisco Bug ID [CSCin82407](#). ([registered](#)) customers only.

A second vulnerability exists in a feature introduced in IOS 12.3(8)T where an ISAKMP profile can be assigned to a remote access peer based on the certificate the peer uses during IKE negotiation. If the ISAKMP profile mandates XAUTH (AAA authentication and authorization lists are configured in the profile), then the peer must perform XAUTH authentication after Phase 1 negotiation.

A vulnerability exists where the ISAKMP profile is assigned but the attributes that are configured in the ISAKMP profile are not processed. This can result in a situation where both the VPN client and VPN server are expecting to hear something from the other end of the connection. Normally this deadlock will be broken by idle timers tearing down the SA, but it is possible for a malicious client to propose Phase 2 negotiation during this time which may allow for the IPsec SA to be fully established.

This issue only affects ISAKMP profiles matched by certificate maps. Configurations with certificate maps configured will contain the commands:

```
crypto isakmp profile <profilename>
  match certificate <mapname>
```

This vulnerability is documented as Cisco Bug ID [CSCeg00277](#). ([registered](#)) customers only.

## Impact

Successful exploitation may result in the affected device allowing an unauthorized user to complete authentication and access network resources.

# Software Versions and Fixes

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. 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 further information on the terms "Rebuild" and "Maintenance" please consult the following URL:

<http://www.cisco.com/warp/public/620/1.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.

Major Release	Availability of Repaired Releases	
Affected 12.2–Based Release	Rebuild	Maintenance
12.2B	Migrate to 12.3(4)T8 or later	
12.2BC	12.2(15)BC1f	
	12.2(15)BC2e	
12.2BX	Vulnerable, contact TAC	
12.2BY	Migrate to 12.3(4)T8 or later	
12.2BZ	Vulnerable, contact TAC	
12.2CX	Migrate to 12.3(9a)BC	
12.2CY	Migrate to 12.2(15)BC1f or 12.2(15)BC2e	
12.2CZ	12.2(15)CZ1	
12.2JK	12.2(15)JK2	
12.2SU	12.2(14)SU2	
12.2SX	Migrate to 12.2(17d)SXB5	
12.2SXA	Migrate to 12.2(17d)SXB5	
12.2SXB	12.2(17d)SXB5	
12.2SXD	12.2(18)SXD1	
12.2SY	Migrate to 12.2(17d)SXB5	
12.2T	Migrate to 12.3 or later	
12.2XJ	Migrate to 12.3 or later	

12.2XK	Migrate to 12.3 or later
12.2XL	Migrate to 12.3 or later
12.2XM	Migrate to 12.3 or later
12.2XW	Migrate to 12.3 or later
12.2XZ	Migrate to 12.3 or later
12.2YA	12.2(4)YA8
12.2YB	Migrate to 12.3 or later
12.2YD	Migrate to 12.3(8)T5 or later
12.2YF	Migrate to 12.3 or later
12.2YG	Migrate to 12.3 or later
12.2YH	Migrate to 12.3 or later
12.2YJ	Migrate to 12.3 or later
12.2YL	Migrate to 12.3T or later
12.2YM	Migrate to 12.3T or later
12.2YN	Migrate to 12.3T or later
12.2YP	Migrate to 12.3 or later
12.2YQ	Migrate to 12.3(4)T8 or later
12.2YR	Migrate to 12.3(4)T8 or later
12.2YT	Migrate to 12.3 or later
12.2YU	Migrate to 12.3T or later
12.2YV	Migrate to 12.3(4)T8 or later
12.2YW	Migrate to 12.3T or later
12.2YX	Migrate to 12.2(14)SU2 or later
12.2YY	Migrate to 12.3T or later
12.2ZB	Migrate to 12.3T or later
12.2ZC	Migrate to 12.3T or later
12.2ZD	Migrate to 12.3(14)T
12.2ZE	Migrate to 12.3 or later
12.2ZF	Migrate to 12.3(4)T8 or later
12.2ZG	Migrate to 12.3(4)T8 or later
12.2ZH	12.2(13)ZH5
12.2ZJ	Migrate to 12.3T or later
12.2ZK	Contact TAC
12.2ZL	12.2(15)ZL2 available TBD
12.2ZN	Migrate to 12.3T or later
12.2ZP	Contact TAC

Affected 12.3–Based Release	Rebuild	Maintenance
12.3	12.3(6e)	
	12.3(9c)	
	12.3(10a)	
		12.3(12)
12.3B	12.3(5a)B3	
12.3BC	12.3(9a)BC	
12.3BW	Migrate to 12.3(7)T6 or later	
12.3T	12.3(2)T9	
	12.3(4)T8	
	12.3(7)T7	
	12.3(8)T5	
	12.3(11)T2	
		12.3(14)T
12.3XA	12.3(2)XA3 available TBD	
12.3XB	Migrate to 12.3(8)T5 or later	
12.3XC	12.3(2)XC3 available TBD	
12.3XD	12.3(4)XD4	
12.3XE	12.3(2)XE1	
12.3XF	Migrate to 12.3(11)T2 or later	
12.3XG	12.3(4)XG2	
12.3XH	Migrate to 12.3(11)T2 or later	
12.3XI	Contact TAC	
12.3XJ	Contact TAC	
12.3XK	Migrate to 12.3(11)T2 or later	
12.3XL		12.3(11)XL
12.3XM	Migrate to 12.3(14)T or later	
12.3XN	Migrate to 12.3(14)T or later	
12.3XQ	12.3(4)XQ1	
12.3XR	12.3(7)XR3	
12.3XS	12.3(7)XS2	
12.3XT	Contact TAC	
12.3XU	12.3(8)XU3	
12.3XW	Contact TAC	

12.3XX	12.3(8)XX1	
12.3XY	Migrate to 12.3(14)T	
12.3YA	12.3(8)YA1	
12.3YC	12.3(8)YC1	
12.3YD		12.3(8)YD
12.3YF		12.3(11)YF
12.3YG		12.3(8)YG1
12.3YH		12.3(8)YH
12.3YI		12.3(8)YI available TBD
12.3YJ		12.3(11)YJ
12.3YK		12.3(11)YK

## Workarounds

The effectiveness of any workaround is dependent on specific deployment scenarios 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.

## Using Strong Group Passwords

Because the preshared group password (also referred to as the group key) must be known by an attacker, the use of a best practice to deploy strong preshared group keys may mitigate a brute-force attack against this group key.

The preshared key can be changed by using the following configuration commands:

```
Router(config)#crypto isakmp client configuration group <group-name>
Router(config)#key <key>
```

## 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.

## 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 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.

## 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/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

## Exploitation and Public Announcements

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

Both vulnerabilities were reported by Cisco customers

## 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.

## Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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.

## Revision History

Revision 1.0	2005-April-6	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](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>.

---

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

---

Updated: Apr 06, 2005

Document ID: 64424

---