

# Cisco Security Notice: Cisco Response to Internet Key Exchange Issue

Document ID: 42302

## Revision 1.1

For Public Release 2003 April 23

Last Updated 2004 July 19

---

Please provide your feedback on this document.

---

**Summary**  
**Details**  
**Cisco Security Procedures**

---

## Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

## Details

The original report is located at <http://www.securityfocus.com/archive/1/319487> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/319529> .

```
To: BugTraq
Subject: Re: Cracking preshared keys
Date: Apr 23 2003 7:46PM
Author: Damir Rajnovic <gaus cisco com>
Message-ID: <4.3.2.7.2.20030423203906.06148110@ca-uk-fs.cisco.com>
In-Reply-To: <5.0.2.1.2.20030423113449.02cb2340@172.31.1.10>
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

```
This is in response to the mail of mthumann ernw de from ERNW GmbH
posted on 2003-Apr-23:
```

```
At 11:35 23/04/2003 +0100, Michael Thumann wrote:
>we would like to announce the publication of a proof of concept paper
>'PSK cracking using IKE Aggressive Mode'. Paper can be downloaded from
>www.ernw.de/download/pskattack.pdf
```

```
The mail itself can be found at
http://www.securityfocus.com/archive/1/319487
```

This text can be found at  
<http://www.cisco.com/warp/public/707/cisco-sn-20030422-ike.html>

IKE (Internet Key Exchange) is used during Phase 1 and Phase 2 of establishing an IPsec connection. Phase 1 is where the two ISA KMP (Internet Security Association and Key Management Protocol) peers establish a secure, authenticated channel with which to communicate. This is called the ISAKMP Security Association (SA). "Main Mode" and "Aggressive Mode" each accomplish a Phase 1 exchange. Each generates authenticated keying material from an ephemeral Diffie-Hellman exchange. Every participant in IKE must possess a key which may be either pre-shared (PSK) or a public key. There are inherent risks to configurations that use pre-shared keys which are exaggerated when Aggressive Mode is used.

When responding to IPsec session initialization, Cisco IOS® software may use Aggressive Mode even if it has not been explicitly configured to do so. Cisco IOS software initially tries to negotiate using Main Mode but, failing that, resorts to Aggressive Mode.

Using Aggressive Mode with pre-shared keys is the least secure option. In this particular scenario, it is possible for an attacker to gather all necessary information in order to mount an off-line dictionary (brute force) attack on the pre-shared keys. The detailed analysis of the attack is given in the article by John Pliam. The article is located at <http://www.vpnc.org/ietf-ipsec/99.ipsec/msg01451.html>. Although this article is about Aggressive Mode, the thread referenced below also contains references to Main Mode.

Please note that this attack method has been known and discussed within the IETF IPsec Working Group. You can find the thread at <http://www.vpnc.org/ietf-ipsec/99.ipsec/thrd2.html#01451>

(Subject: Weak authentication in Xauth and IKE). The IPsec Working Group has understood and acknowledged this attack avenue, but has deemed that this is an acceptable risk. There are public information-gathering tools which target IPsec session initiation and brute-force the pre-shared key. One of them can be found at <http://ikecrack.sourceforge.net/>

The most exposed users are those who use IPsec to connect to internal resources across a hostile network (for example, a sales person visiting a customer). The entire session may be intercepted on the hostile network and manipulated while the user is unaware of such activity. Note that the recorded session (the one that was used to discover PSK) cannot be decrypted. It is still protected by the ephemeral Diffie-Hellman key exchange. An adversary can either use a pre-shared key to impersonate a trusted user and connect to the protected network, or it can mount an active Man-in-The-Middle (MitM) attack on any new session. Another high-risk scenario is group pre-shared keys, that is, a single shared key is assigned to all dial-in users.

Please note that the same class of attack is possible even if Xauth (Extended Authentication) is used. This is because Xauth is performed after Phase 1 is completed and, for this attack, an adversary needs only a packet from Phase 1. Furthermore, after the pre-shared key has been discovered, an adversary can mount an active MitM attack on Xauth. The outcome depends on the exact authentication method used in Xauth.

Mitigation of this risk is to use, as long as practical, strong pre-shared keys, and to change them frequently. In Cisco IOS software,

the PSK can be up to 128 characters in length. According to some estimates, one character carries from 1.3 to up to 4 bits of entropy. This means that the password can have, at maximum, anywhere from 166 to 512 bits of entropy. The length of the PSK should be determined by your security policy.

## 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>.

---

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

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

---

Updated: Jul 19, 2004

Document ID: 42302

---