

Cisco Security Notice: Cisco IPsec VPN Implementation Group Password Usage Vulnerability

Document ID: 50600

Revision 2.2

Last Updated 2006 January 26 23:30 UTC (GMT)

For Public Release 2004 April 15 1600 UTC (GMT)

Please provide your feedback on this document.

[Summary](#)
[Details](#)
[Symptoms](#)
[Workarounds](#)
Status of This Notice: FINAL
[Revision History](#)
[Cisco Security Procedures](#)
[Related Information](#)

Summary

This Security Notice is being released due to the new information received by Cisco PSIRT regarding the Cisco IPsec VPN implementation, Group Password Usage Vulnerability.

This is also a follow-up to an email thread that appeared on the Bugtraq mailing list in December 2003 which can be found at <http://www.securityfocus.com/archive/1/347351> .

This notice will be posted at <http://www.cisco.com/warp/public/707/cisco-sn-20040415-grppass.shtml>.

Details

Proof of Concept code now exists for:

- **Recovering the Group Password** The Group Password used by the Cisco Internet Protocol Security (IPsec) virtual private network (VPN) client is scrambled on the hard drive, but unscrambled in memory. This password can now be recovered on both the Linux and Microsoft Windows platform implementations of the Cisco IPsec VPN client. This vulnerability is documented in the Cisco Bug Toolkit as Bug ID CSCed41329 (registered customers only).
 - ◆ The Linux implementation vulnerability was reported by Karl Gaissmaier, University of Ulm, Germany.
 - ◆ The Microsoft Windows implementation vulnerability was reported by Jonas Eriksson and Nicholas Kathmann.
- **Man In The Middle (MITM) attack to emulate a VPN head end server for stealing valid user names and passwords or hijacking connections using a previously recovered Group Password**

This vulnerability exists whenever Group Passwords are used as the pre-shared key during Internet Key Exchange (IKE) Phase 1 in the XAUTH protocol. The user name and password in XAUTH are transmitted over the network only encrypted by the Phase 1 IKE security association (SA) which in this case are derived from the Group Password. Anyone in possession of the Group Passwords will have the ability to either hijack a connection from a valid user, or pose as a VPN head end for stealing user names and passwords.

In the e-mail thread on Bugtraq, it was mentioned that Cisco may be looking at implementing Challenge/Response Authentication of Cryptographic Keys (CRACK) as an alternate to XAUTH. This information was incorrect and Cisco does not plan to implement the CRACK authentication method.

The new version of the IKE protocol, IKE version 2 (IKEv2), described in RFC 4306, performs mutual authentication between two IPsec parties.

Cisco is planning to add support for IKEv2 in upcoming versions of the Cisco IOS, the Adaptive Security Appliance (ASA), and the PIX Security Appliance software.

For the Cisco VPN 3000 Concentrator, Cisco VPN Client (software client) and Cisco VPN 3002 Hardware Client, Cisco has implemented a feature that is based on the expired IETF draft 'A Hybrid Authentication Mode for IKE' published in August of 2000.

Cisco's solution extends the Hybrid Auth model by additionally requiring a group pre-shared key for VPN group identification. The group pre-shared key is used solely to associate users with their appropriate VPN groups, followed by the XAUTH exchange that then authenticates the user.

The MITM attack vulnerability described in this document is no longer possible because of the additional digital signature that binds the keying material to the Cisco VPN 3000 Concentrator's digital certificate.

This feature, called "Mutual Group Authentication", first appeared in release 4.0.5 of the Cisco VPN software (client and concentrator) and is documented in the release notes for this version:

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/rel405/405clnt.htm#wp1375735>

Hybrid Authentication mode is a two stage process that allows the asymmetric use of digital certificates between the client and the head end server. The first stage is used to authenticate the head end server by the client and is based on the IKE Phase 1 exchange where in the client verifies the authenticity of the head end server's certificate. The second stage authenticates the client by the head end server and is based on a Transaction Exchange (IKECFG) using the mechanism described in the XAUTH protocol. Pre-shared keys are not used.

Cisco recommends that the new Mutual Group Authentication feature be used in conjunction with the Certificate Distinguished Name (DN) Group Matching feature for additional security. This feature has been available since version 3.6.1 of the VPN 3000 concentrator:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/prod_release_note09186a00801fc7a4.html#192439

Symptoms

There are no symptoms for this issue.

Workarounds

The MITM attack vulnerability described in this document and in the original Bugtraq post is no longer possible when using the new "Mutual Group Authentication" feature because of the additional digital signature that binds the keying material to the Cisco VPN 3000 Concentrator's digital certificate.

To avoid the potential exploitation of the MITM attack vulnerability described here, Cisco PSIRT recommends that customers deploy the new "Mutual Group Authentication" feature and carefully evaluate the risks of deploying Group Password based authentication schemes.

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.

Revision History

Revision 2.2	2006-January-26	Clarified plans to support IKE version 2 in Cisco products. Changed status of advisory to FINAL.
Revision 2.1	2004-October-26	Stated in the Workarounds section that the MITM attack is no longer possible when the new "Mutual Group Authentication" feature is used.
Revision 2.0	2004-September-28	Added information about software images for the Cisco VPN 3000 concentrator, Cisco VPN Client (software client) and Cisco VPN 3002 hardware client that implement a new hybrid authentication mode.
Revision 1.0	2004-April-15	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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Related Information

- **SAFE VPN IPsec Virtual Private Networks in Depth –**
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a0
– refer to the Identity and IPsec Access Control under Architecture Overview section.
 - **Deploying Cisco IOS Security with a Public–Key Infrastructure –**
http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/pkdpdpy_wp.htm
 - **A Hybrid Authentication Mode for IKE –**
<http://www.ietf.org/proceedings/00dec/I-D/draft-ietf-ipsec-isakmp-hybrid-auth-05.txt>
 - **Cisco Response to Internet Key Exchange Issue –**
<http://www.cisco.com/warp/public/707/cisco-sn-20030422-ike.html>
-

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

Updated: Jan 26, 2006

Document ID: 50600
