

Securiteam: [NEWS] Cisco IPsec VPN Implementation Group Password Usage Vulnerability

[NEWS] Cisco IPsec VPN Implementation Group Password Usage Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0064.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/18/04

To: list@securiteam.com

Date: 18 Apr 2004 16:26:11 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Cisco IPsec VPN Implementation Group Password Usage Vulnerability

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.

DETAILS

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.

* The Linux implementation vulnerability was reported by Karl Gaissmaier, University of Ulm, Germany.

Securiteam: [NEWS] Cisco IPsec VPN Implementation Group Password Usage Vulnerability

* 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 might 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.

Cisco is working on implementing IKEv2 with an estimated release date in the fourth quarter of the calendar year 2005.

For the Cisco VPN 3000 Concentrator, Cisco VPN Client (software client) and Cisco VPN 3002 Hardware Client, Cisco is in the process of implementing 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 will be used solely to associate users with their appropriate VPN groups, followed by the XAUTH exchange that will then authenticate the user.

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

This feature is estimated to ship in the third quarter of the calendar year 2004.

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.

Workarounds:

No workarounds exist for the vulnerabilities documented in this Notice.

Securiteam: [NEWS] Cisco IPsec VPN Implementation Group Password Usage Vulnerability

To avoid the potential exploitation because of these vulnerabilities Cisco PSIRT recommends customer deploy Public Key Infrastructure (PKI) and carefully evaluate the risks of deploying Group Password based authentication schemes.

ADDITIONAL INFORMATION

Related Information:

SAFE VPN IPsec Virtual Private Networks in Depth –

<http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2c.html>
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.html

– 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/pkdpw_wp.htm>
http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/pkdpw_wp.htm

A Hybrid Authentication Mode for IKE –

<<http://www.ietf.org/proceedings/00dec/I-D/draft-ietf-ipsec-isakmp-hybrid-auth-05.txt>>
<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>>
<http://www.cisco.com/warp/public/707/cisco-sn-20030422-ike.html>

The information has been provided by <<mailto:psirt@cisco.com>> Cisco Systems Product Security Incident Response Team.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.