

CERT-FI and NISCC Joint Vulnerability Advisory ISAKMP

Multiple Vulnerability Issues in Implementation of ISAKMP Protocol

Version Information

Advisory Reference	CERT-FI: 7710 NISCC: 273756/NISCC/ISAKMP
Release Date	14 November 2005
Last Revision	3 January 2006
Version Number	1.8

Acknowledgement

This issue was identified by the Oulu University Secure Programming Group (OUSPG) from the University of Oulu in Finland.

What is Affected?

The vulnerabilities described in this advisory affect the Internet Security Association and Key Management Protocol (ISAKMP), which is used to provide associations for other security protocols.

Internet Key Exchange version 1 (IKEv1), a derivate of ISAKMP, is an important part of IPsec. IPsec is widely used to secure exchange of packets at the IP layer and mostly used to implement Virtual Private Networks (VPNs). In addition to dedicated VPN-products, ISAKMP/IKE support has also been included in many operating system distribution packages and some firewall products.

Impact

These flaws may expose Denial-of-Service conditions, format string vulnerabilities, and buffer overflows. In some cases, it may be possible for an attacker to execute code.

ISAKMP/IKE client applications may be harder to attack than server applications because in some cases, it may be required that clients initialise the negotiation.

Severity

The severity of these vulnerabilities varies by vendor, please see the "Vendor Information" section below for further information or contact your vendor for product specific information.

Summary

During 2002 OUSPG discovered a number of implementation specific vulnerabilities in the Simple Network Management Protocol (SNMP). Further work has been done to identify implementation specific vulnerabilities in related protocols that are used in critical infrastructure. The ISAKMP protocol, an important part of the IPsec protocol which is widely used in critical infrastructure, was studied as part of this program of work.

OUSPG has developed a PROTOS ISAKMP Test Suite for IKEv1 Phase 1 and employed it to validate their findings against a number of products from different vendors. CERT-FI and NISCC have contacted multiple vendors whose products employ ISAKMP/IKE and provided them with the test tool to allow them to test their implementations. These vendors' product line covers most of the existing IPsec based VPN-products in the market.

The ISAKMP Test Suite can be downloaded from the URL below:

<http://www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp/>

Details

The ISAKMP protocol is an international standard protocol, published by the Internet Engineering Task Force (IETF). ISAKMP is designed to establish, negotiate, modify and delete Security Associations (SA). SAs contain all the information required for execution of various network security services. ISAKMP provides a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism. IKEv1, a derivate of ISAKMP, is a key protocol in the Internet Security Architecture (IPsec). IKEv1 is the most widely used version of the Internet Key Exchange protocol.

Please note that the OUSPG PROTOS ISAKMP Test Suite does not test Internet Key Exchange version 2 (IKEv2).

ISAKMP consists of two phases. In phase 1, the two parties negotiate a SA to agree on how to protect the traffic in the next phase. In phase 2 keying material is derived and the policy to share it is negotiated. In this way, security associations for other security protocols are established.

Multiple ISAKMP implementations behave in anomalous way when they receive and handle ISAKMP Phase 1 packets with invalid and/or abnormal contents. By applying the OUSPG PROTOS ISAKMP Test Suite to a variety of products, several vulnerabilities can be revealed that can have varying effects.

Mitigation

The following suggestions are recommended as methods to mitigate against the issues discussed in this advisory:

- If possible, use packet filter and accept ISAKMP negotiations only from trusted IP-addresses
- Avoid using "aggressive mode*" in phase 1

[*In "aggressive mode", fewer exchanges are made and with fewer packets during the negotiation stage. The weakness of using this mode is that both sides have exchanged information before there is a secure channel.]

Solution

Please refer to the 'Vendor Information' section of this advisory for platform specific remediation.

Vendor Information

The following vendors have provided information about how their products are affected by this vulnerability.

Please note that [JPCERT/CC](http://www.jpcert/cc) have released a Japanese language advisory for this vulnerability which contains additional information regarding Japanese vendors. This advisory is available at: <http://jvn.jp/niscc/NISCC-273756/index.html>

3Com

ADTRAN, Inc.

Aruba

Barron McCann

Check Point

Cisco

Entrust

Hitachi

HP

IBM

Intoto Inc

Juniper Networks, Inc

Microsoft

Mitel Corporation

NEC

Nortel

Secgo

SonicWALL

Stonesoft Corp

strongSwan

Sun

TeamF1 Inc

3Com

3Com is investigating the reported vulnerabilities in ISAKMP to determine if any devices in our product line are affected. We will provide updated status at the conclusion of our investigation.

ADTRAN, Inc.

ADTRAN, Inc. has published a security advisory regarding the vulnerabilities identified by CERT-FI: 7710 and NISCC: 273756/NISCC/ISAKMP as they pertain to ADTRAN NetVanta VPN-enabled products. This advisory is available at the following URL: <http://www2.adtran.com/support/isakmp>.

Aruba

Aruba Networks have published an advisory about this issue. The advisory is available at:

<http://www.arubanetworks.com/support/wsirt/alerts/aid-11142005.asc>

Barron McCann

After reading the CERT-FI and NISCC Joint Vulnerability Advisory report on ISAKMP vulnerabilities, we have determined that none of the products in the X-Kryptor line are affected by this issue. We have prepared a statement which is available on our website.

<http://www.bemac.com/ISec/s1pressrelease.asp?PRID=131&S1ID=2>

Check Point

Check Point has published an advisory about this issue. The advisory is available on:

<http://secureknowledge.us.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk31316>

Cisco

Cisco Systems has released a security advisory addressing the vulnerabilities identified by CERT-FI: 7710 and NISCC: 273756/NISCC/ISAKMP across its entire product line.

The advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20051114-ipsec.shtml>

For up-to-date information on security vulnerabilities in Cisco Systems products, visit: <http://www.cisco.com/go/psirt/>

Entrust

Entrust has examined the vulnerabilities disclosed in NISCC Vulnerability #273756 and issued security bulletin E05-009. Customers and partners can obtain further information at:

<https://www.entrust.com/trustedcare/troubleshooting/e05-009.htm>

or by contacting Entrust Customer Support.

Hitachi

Hitachi

=====

AlaxalA AX2000R, Hitachi GR2000 B and Hitachi HI-UX/WE2 are NOT vulnerable to the issue described in NISCC Vulnerability 273756.

HP

HP has released the following Security Bulletins for this issue:

HPSBUX02076 SSRT5979 - HP-UX Running IPsec Remote Denial of Service (DoS)

HPSBPI02078 SSRT5979 - HP Jetdirect 635n IPv6/IPsec Print Server (J7961A) Remote Denial of Service (DoS)

These bulletins are available at: <http://itrc.hp.com>

HP Tru64 Unix is not vulnerable.

IBM

At this time is believed that the AIX Operating System is NOT vulnerable to the issues described in NISCC Vulnerability 273756.

IBM recommends that IPsec be configured to use IKE in main mode. IPsec on AIX also supports filters. By configuring IPsec to use static filter rules, an AIX host will only process IPsec packets from trusted hosts. More information about using IKE in main mode and using IPsec filters can be found in the AIX Security Guide.

Intoto Inc

Intoto's engineering team ran all 5000 vulnerability tests on its most recent version of the Intoto iGateway VPN product using the c09-isakmp

tool. It was observed that iGateway VPN did not show any vulnerabilities documented in this advisory during or after the test.

Juniper Networks, Inc

Bulletin Number: PSN-2005-11-007

Title: IKE version 1 vulnerability issues resulting from OUSPG ISAKMP Test Suite (NISCC/ISAKMP/273756)

Products Affected: All Juniper Networks M/T/J/E-series routers.

Platforms Affected: JUNOS Security / JUNOSe Security

Issue:

The University of Oulu Security Programming Group (OUSPG) has developed an ISAKMP Test Suite for IKE version 1 Phase 1, a key component of the IPsec encryption and security protocol. The IKE protocol implementation in JUNOS and JUNOSe software is vulnerable to certain test cases in the test suite provided by OUSPG.

This issue is tracked internally as CQ/68020 for JUNOSe software and PR/61076 and PR/61779 for JUNOS software.

Solution:

Changes have been made in the JUNOSe and JUNOS software that resolve the potential vulnerability exposed by the OUSPG ISAKMP/IKE test suite.

In addition, Juniper Networks agrees with the mitigation recommendations in the NISCC advisory.

Solution Implementation:

The following JUNOSe software (used on E-series routers) releases contain modified code that provides fixes for the IKE security protocol: 5-2-4p0-8, 5-2-5, 5-3-4p0-5, 6-0-2p0-5, 6-0-3, 6-1-1p0-7, 6-1-2, 7-0-0p0-1, 7-0-1, 7-1-0.

All JUNOS software (for M/T/J-series routers) for Releases 6.4 and later releases built on or after July 28, 2005 contains modified code that provides fixes for the IKE security protocol.

Risk Level: High

Risk Assessment:

Juniper Networks JUNOS and JUNOSe software is susceptible to certain IPSec ISAKMP/IKE vulnerabilities as exposed by the OUSPG ISAKMP/IKE test suite. Risk assessment is high for Juniper Networks E/M/T/J-series routers.

Microsoft

Microsoft has reviewed the report and has determined that there are no known Microsoft products that are affected by this issue.

Mitel Corporation

Not vulnerable, with the possible exception of the 6042 Managed VPN product that is still under investigation. If any issues are found an advisory will be posted to <http://www.mitel.com/security> and if you have concerns you may e-mail them to security@mitel.com.

NEC

Some of NEC products are affected by this vulnerability.

- For more detail.

<http://www.sw.nec.co.jp/psirt/index.html> (only in Japanese)

- We continue to investigate our products.

Nortel

Nortel has published a Security Advisory on these issues. The advisory is available at the following address, reference number 2005006429:

<http://www.nortel.com/securityadvisories>

Secgo

CERT-FI has found problems in multiple IKEv1 implementations. These issues affect certain versions of Secgo Crypto IP gateway and client products and are partly caused by defects in a third party toolkit code that Secgo is using.

Successful exploitation of these problems may cause the software to crash or a buffer overflow situation. If you have Secgo Crypto IP Gateway or Client version 3.2.26 or earlier, you should upgrade immediately.

See more detailed information on the problem at:

http://www.secgo.com/newsletter/20051114/CIP517_description.txt

SonicWALL

SonicWALL is investigating the ISAKMP vulnerabilities to determine which devices in our product line are affected. We will provide updated status as our investigation progresses.

Stonesoft Corp

Stonesoft has published a Security Advisory on these issues. The advisory is available at Stonesoft's web site:

http://www.stonesoft.com/support/Security_Advisories/14112005.html

strongSwan

The Linux strongSwan IPsec software is NOT vulnerable to any of the malformed IKE packets and sequences generated by the 5000 test cases. The subset of IKE Aggressive Mode test cases is not an issue at all, simply because strongSwan has not implemented this potentially dangerous mode.

Sun

Sun acknowledges that there is a security issue in the Solaris ISAKMP daemon which is revealed by the test suite described in NISCC notice #273756.

Sun has published Sun Alert 102040 describing the Sun-specific impact, contributing factors, and resolution. This is available at the following URL:

<http://sunsolve.sun.com/search/document.do?assetkey=3D1-26-102040-1=20>

The Solaris IPSec implementation does not support aggressive mode in phase 1 negotiations, meaning that no action need be taken to implement the second mitigation method recommended in the NISCC's advisory.

TeamF1 Inc

TeamF1's V-IPSecure embedded IPsec/IKE software is NOT affected by this ISAKMP vulnerability. Please contact us at <http://www.TeamF1.com/contactus.htm> for more information.

Credits

CERT-FI and the NISCC Vulnerability Team would like to thank OUSPG for informing us of the problems and making the test suite available to vendors.

CERT-FI and the NISCC Vulnerability Team would also like to thank the vendors for their co-operation in handling this vulnerability and to JPCERT/CC for co-ordinating this issue in Japan.

References

CERT-FI Advisory:

<http://www.ficora.fi/englanti/document/ISAKMP.pdf>

Contact Information

CERT-FI Vulnerability Coordination can be contacted as follows:

Email	vulncoord@ficora.fi <i>(Please quote the advisory reference in the subject line.)</i>
Telephone	+358-9-6966510 Monday - Friday 08:00 - 16:15 (EET-DST: UTC+3, EET: UTC+2)
Fax	+358-9-6966515
Post	Vulnerability Coordination FICORA/CERT-FI P.O. Box 313 FI-00181 Helsinki FINLAND

CERT-FI encourages those who wish to communicate via email to make use of their PGP key. This is available from <http://www.ficora.fi/suomi/tietoturva/VULNCOORD.asc>.

The NISCC Vulnerability Management Team can be contacted as follows:

Email	vulteam@nisc.gov.uk <i>(Please quote the advisory reference in the subject line.)</i>
Telephone	+44 (0)870 487 0748 Extension 4511 <i>(Monday to Friday 08:30 - 17:00)</i>

Fax	+44 (0)870 487 0749
Post	Vulnerability Management Team NISCC PO Box 832 London SW1P 1BG United Kingdom

We encourage those who wish to communicate via email to make use of our PGP key. This is available from <http://www.niscc.gov.uk/niscc/publicKey2-en.pop>.

Please note that UK government protectively marked material should not be sent to the email address above.

If you wish to be added to our email distribution list, please email your request to uniras@niscc.gov.uk.

What is NISCC?

For further information regarding the Finnish national CERT team, CERT-FI, please visit: <http://www.ficora.fi/englanti/tietoturva/cert.htm>.

For further information regarding the UK National Infrastructure Security Co-ordination Centre, please visit <http://www.niscc.gov.uk>.

Reference to any specific commercial product, process or service by trade name, trademark manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this notice shall not be used for advertising or product endorsement purposes.

Neither shall NISCC accept responsibility for any errors or omissions contained within this advisory. In particular, they shall not be liable for any loss or damage whatsoever, arising from or in connection with the usage of information contained within this notice.

© 2005 Crown Copyright

Revision History

14 Nov 2005	Initial release (1.0)
14 Nov 2005	Added vendor statements and updated JPCERT URL (1.1)
15 Nov 2005	Added vendor statements from Sun and Check Point (1.2)

16 Nov 2005	Added vendor statement from Aruba and updated statement from Sun (1.3)
16 Nov 2005	Added vendor statement from Nortel (1.4)
17 Nov 2005	Added vendor statements from Barron McCann, HP and SonicWALL (1.5)
8 Dec 2005	Added vendor statement for ADTRAN, Inc. (1.6)
19 Dec 2005	Added vendor statement for NEC (1.7)
3 Jan 2006	Added vendor statement for Hitachi (1.8)

<End of NISCC Vulnerability Advisory>