

# NISCC Vulnerability Advisory 004033/NISCC/IPSEC

## Vulnerability Issues with IPsec Configurations

### Version Information

Advisory Reference	004033/NISCC/IPSEC
Release Date	9 May 2005
Last Revision	16 May 2005
Version Number	1.3

### What is Affected?

Potentially any configuration of IPsec that uses Encapsulating Security Payload (ESP) in tunnel mode with confidentiality only, or with integrity protection being provided by a higher layer protocol. Some configurations using AH to provide integrity protection are also vulnerable.

### Impact

If exploited, it is possible for an active attacker to obtain the plaintext version of the IPsec-protected communications using only moderate effort.

### Severity

This is rated as high.

### Summary

IP Security (IPsec) is a set of protocols developed by the Internet Engineering Task Force (IETF) to support secure exchange of packets at the IP layer; IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

Three attacks that apply to certain configurations of IPsec have been identified. These configurations use Encapsulating Security Payload (ESP) in tunnel mode with confidentiality only, or with integrity protection being provided by a higher layer protocol. Some configurations using AH to provide integrity protection are also vulnerable. In these configurations, an attacker can modify sections of the IPsec packet, causing either the cleartext inner packet to be redirected or a network host to generate an error message. In the latter case, these errors are relayed via the Internet Control

Message Protocol (ICMP); because of the design of ICMP, these messages directly reveal segments of the header and payload of the inner datagram in cleartext. An attacker who can intercept the ICMP messages can then retrieve plaintext data. The attacks have been implemented and demonstrated to work under realistic conditions.

## **Details**

*CVE number: CAN-2005-0039*

IPsec consists of several separate protocols; these include:

- Authentication Header (AH): provides authenticity guarantees for packets, by attaching strong cryptographic checksum to packets.
- Encapsulating Security Payload (ESP): provides confidentiality guarantees for packets, by encrypting packets with encryption algorithms. ESP also provides optional authentication services for packets.
- Internet Key Exchange (IKE): provide ways to securely negotiate shared keys.

AH and ESP has two modes of use: transport mode and tunnel mode. With ESP in tunnel mode, an IP packet (called the inner packet) is encrypted in its entirety and is used to form the payload of a new packet (called the outer packet); ESP typically uses CBC-mode encryption to provide confidentiality. However, without some form of integrity protection, CBC-mode encrypted data is vulnerable to modification by an active attacker.

By making careful modifications to selected portions of the payload of the outer packet, an attacker can effect controlled changes to the header of the inner (encrypted) packet. The modified inner packet is subsequently processed by the IP software on the receiving security gateway or the endpoint host; the inner packet, in cleartext form, may be redirected or certain error messages may be produced and communicated by ICMP. Because of the design of ICMP, these messages directly reveal cleartext segments of the header and payload of the inner packet. If these messages can be intercepted by an attacker, then plaintext data is revealed.

Attacks exploiting these vulnerabilities rely on the following:

- Exploitation of the well-known bit flipping weakness of CBC mode encryption.

- Lack of integrity protection for inner packets.
- Interaction between IPsec processing and IP processing on security gateways and end hosts.

These attacks can be fully automated so as to recover the entire contents of multiple IPsec-protected inner packets.

In more detail, the three identified attacks on ESP in tunnel mode when integrity protection is not present work as follows:

### 1. Destination Address Rewriting

- An attacker modifies the destination IP address of the encrypted (inner) packet by bit-flipping in the payload of the outer packet.
- The security gateway decrypts the outer payload to recover the (modified) inner packet.
- The gateway then routes the inner packet according to its (modified) destination IP address.
- If successful, the "plaintext" inner datagram arrives at a host of the attacker's choice.

### 2. IP Options

- An attacker modifies the header length of the encrypted (inner) packet by bit-flipping in the payload of the outer packet.
- The security gateway decrypts the outer payload to recover the (modified) inner packet.
- The gateway then performs IP options processing on the inner packet because of the modified header length, with the first part of the inner payload being interpreted as options bytes.
- With some probability, options processing will result in the generation of an ICMP "parameter problem" message.
- The ICMP message is routed to the now modified source address of the inner packet.

- An attacker intercepts the ICMP message and retrieves the "plaintext" payload of the inner packet.

### 3. Protocol Field

- An attacker modifies the protocol field and source address field of the encrypted (inner) packet by bit-flipping in the payload of the outer packet.
- The security gateway decrypts the outer payload to recover the (modified) inner packet.
- The gateway forwards the inner packet to the intended recipient.
- The intended recipient inspects the protocol field of the inner packet and generates an ICMP "protocol unreachable" message.
- The ICMP message is routed to the now modified source address of the inner packet.
- An attacker intercepts the ICMP message and retrieves the "plaintext" payload of the inner packet

The attacks are probabilistic in nature and may need to be iterated many times in a first phase in order to be successful. Once this first phase is complete, the results can be reused to efficiently recover the contents of further inner packets.

Naturally, the attacker must be able to intercept traffic passing between the security gateways in order to mount the attacks. For the second and third attacks to be successful, the attacker must be able to intercept the relevant ICMP messages. Variants of these attacks in which the destination of the ICMP messages can be controlled by the attacker are also possible.

### **Solution**

Any of the following methods can be used to rectify this issue:

1. Configure ESP to use both confidentiality and integrity protection. This is the recommended solution.
2. Use the AH protocol alongside ESP to provide integrity protection. However, this must be done carefully: for

example, the configuration where AH in transport mode is applied end-to-end and tunnelled inside ESP is still vulnerable.

3. Remove the error reporting by restricting the generation of ICMP messages or by filtering these messages at a firewall or security gateway.

## Credits

The NISCC Vulnerability Team would like to thank all vendors for their co-operation with the handling of this vulnerability.

NISCC would also like to thank JPCERT/CC for their assistance in co-ordinating this issue with Japanese vendors.

## Vendor Information

The following vendors have provided information about how their products are affected by these vulnerabilities.

*Please note that [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-004033/index.html>.*

Cisco Systems, Inc

Hitachi

IBM

Juniper Networks

Nortel

Symantec Corp

### Cisco Systems, Inc

The attacks described are attacks against IPsec in tunnel mode without authentication configured.

Configuring authentication in addition to confidentiality on IPsec tunnels will prohibit the attack, and has been a recommended Cisco best practice.

For Cisco's SAFE Blueprint for IPsec VPNs, consult the following link:

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/net\\_working\\_solutions\\_white\\_paper09186a00801dca2d.shtml](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/net_working_solutions_white_paper09186a00801dca2d.shtml)

Questions can be addressed to [psirt@cisco.com](mailto:psirt@cisco.com).

Hitachi

[VULNERABLE]

Hitachi GR2000 B is vulnerable to this issue.

Please use the AH protocol alongside ESP to provide integrity protection.

[NOT VULNERABLE]

AlaxalA AX series are NOT vulnerable.  
Hitachi HI-UX/WE2 is NOT Vulnerable.

IBM

The AIX Operating System is not vulnerable to the issues described in NISCC advisory 004033.

IBM recommends that IPsec be configured with AH support. IPsec will be configured with AH support if it is configured via SMIT or WebSM. It is possible to configure IPsec without AH support using the gentun command. However, even if IPsec is configured without AH support, AIX is not affected by the vulnerabilities described by NISCC advisory 004033. Future versions of the gentun command will remove the possibility for system administrators to configure IPsec without AH support.

Juniper Networks

Juniper Networks acknowledges that there exists a vulnerability in the IPsec protocol that can be activated through unconventional configuration on M/T/J/E-series routers and ScreenOS based firewalls. Such insecure, vulnerability-enabling configurations are not recommended and are not part of Juniper's default configurations.

Nortel

Nortel has posted a bulletin on this issue at our Technical Support site:

[www.nortel.com/securityadvisories](http://www.nortel.com/securityadvisories)

Symantec Corp

Symantec's IPSEC products provide integrity, authentication and confidentiality and are not vulnerable.

**Contact Information**

The NISCC Vulnerability Management Team can be contacted as follows:

Email	<a href="mailto:vulteam@niscc.gov.uk">vulteam@niscc.gov.uk</a> <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

We encourage those who wish to communicate via email to make use of our PGP key. This is available from <http://www.uniras.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](mailto:uniras@niscc.gov.uk).

### **What is NISCC?**

For further information regarding the UK National Infrastructure Security Co-Ordination Centre, please visit the NISCC web site at: <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**

9 May 2005	Initial Release (1.0)
10 May 2005	Added Nortel's statement (1.1)
11 May 2005	Added Cisco's statement (1.2)
	Added Symantec's statement (1.2)
16 May 2005	Added Juniper's statement (1.3)

<End of NISCC Vulnerability Advisory>