

NISCC Vulnerability Advisory 532967/NISCC/ICMP

Vulnerability Issues in ICMP packets with TCP payloads

Version Information

Advisory Reference	532967/NISCC/ICMP
Release Date	12 April 2005
Last Revision	6 December 2005
Version Number	1.8

What is Affected?

The vulnerabilities described in this advisory affect the TCP (Transmission Control Protocol) by using Internet Control Message Protocol (ICMP) messages that comply with the Internet Engineering Task Force's (IETF's) Requests For Comments (RFCs) for ICMP, including RFC 792 "Internet Control Message Protocol: DARPA Internet Program Protocol Specification" (for IP Version 4), RFC 1122, "Requirements for Internet Hosts -- Communication Layers" and potentially RFC 2463 "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification" (for IP Version 6). The original TCP specification is provided in RFC 793.

ICMP is the control protocol for IP (Internet Protocol), a core network protocol used in the majority of networked computer systems today. Most vendors include support for this protocol in their products and may be impacted to varying degrees. Furthermore any network service or application that relies on a long-lived TCP connection will also be impacted if the host processes ICMP messages in accordance with RFC 1122. For the Source Quench attack the severity will depend on the throughput of the TCP connection; the application may well become unusable.

Severity

The impact of the ICMP TCP reset vulnerability (called "the TCP blind connection-reset vulnerability" in this advisory) varies by vendor and application, but in some deployment scenarios it is likely to be rated medium to high. Please see the 'Vendor Information' section below for further information. Alternatively contact your vendor for product specific information.

If exploited, the TCP blind connection-reset vulnerability could allow an attacker to create a denial-of-service condition against existing TCP connections, resulting in premature session termination. The resulting session termination will affect the application layer, the nature and severity of the effects being dependent on the application layer protocol. The primary dependency is on the tolerance of the network service or application to the loss of a TCP connection.

The Border Gateway Protocol (BGP) is judged to be potentially most affected by this vulnerability. BGP relies on a persistent TCP connection between BGP peers; resetting the connection can result in medium term unavailability due to the need to rebuild routing tables and route flapping. Route flapping may result in route dampening (suppression) if the route flaps occur frequently within a short time interval. The overall impact on BGP is likely to be low to moderate based on the likelihood of successful attack, but could be high if an ICMP implementation does not perform any checks on the ICMP payload.

If an access control list is applied at routers to block packets of ICMP Type 3 codes 2, 3 and 4 then the impact will be low as this measure will successfully mitigate the vulnerability. Anti-spoofing measures can also be of benefit if the attacker spoofs the IP address from where the ICMP packet is sent. Anti-spoofing measures include access control lists to block non-routable IP addresses (see RFCs 1918 and 3330) and Unicast Reverse Path Forwarding (URPF) that checks the consistency of the source IP address with the interface on which the packets are received. See NISCC Technical Note 06/02 "Response to Distributed Denial-of-Service (DDoS) Attacks" for further details.

There is a potential impact on other application protocols such as DNS (Domain Name System) and SSL (Secure Sockets Layer) in the case of zone transfers and ecommerce transactions respectively, but the sessions can be restarted without medium term unavailability problems. In the case of DNS the TCP connections are short lived, so the chance of the vulnerability being exploited is lower than for long lived TCP connections. In the case of SSL it may be difficult to guess the source IP address because it could be dynamically allocated home user address (in the case of Internet banking).

The severity of the related issue of slowing down routers that use Path MTU discovery is also likely to be moderate to high in some vendors' products because RFC 792 and RFC 1191 ("Path MTU discovery") do not specify checking of sequence numbers.

The severity of the spoofing of ICMP Source Quench packets is likely to be moderate to low because the support of routers for Source Quench as a means of congestion control has been deprecated for ten years. RFC 1812 section 5.3.6 states: "As described in Section [4.3.3.3], this document recommends that a router SHOULD NOT send a Source Quench to the sender of the packet that it is discarding. ICMP Source Quench is a very weak mechanism, so it is not necessary for a router to send it, and host software should not use it exclusively as an indicator of congestion." On the other hand, RFC 1122 section 4.2.3.9 states that "TCP MUST react to a Source Quench by slowing transmission on the connection", a statement honoured in a number of TCP implementations. To mitigate Source Quench attacks using spoofed IP addresses in the payload, ICMP Source Quench (ICMP Type 4) messages should not be allowed through routers or through firewalls at the organisational perimeter. It is reasonable to allow routers to block Source Quench packets if their use is deprecated.

Summary

The first issue described in this advisory is the practicability of resetting an established TCP connection by sending suitable ICMP packets that simulate a hard error condition in an existing TCP connection. Hard error conditions are defined in RFC 1122 section 4.2.3.9 and include a number of common ICMP types. An ICMP error packet records the IP header of the packet causing the error as well as the first 64 bits of the TCP header, which consists of the source and destination ports and the sequence number. Many ICMP implementations only check the IP addresses and TCP ports at either end of the connection; they do not check whether the sequence number of the packet is within an acceptable range (see 'Details' section below for characterisation of this range).

It is thus possible in some implementations for an attacker to reset an existing TCP connection by sending a suitably crafted ICMP packet with the correct IP addresses and TCP ports. The target of these denial-of-service attacks is any TCP connection, especially one for which the source port can be identified or guessed. Moreover any application protocol which relies on long term TCP connections and for which the source and destination IP addresses and TCP ports are known or can be easily guessed will be vulnerable to denial-of-service attacks.

A related, subsidiary issue is the potential ability to slow down traffic through hosts that use Path MTU discovery (defined in RFC 1191) by sending forged ICMP Type 3 Code 4 ("Fragmentation

Needed and Don't Fragment was Set") packets that report a (false) low "next-hop MTU" to a host using the Path MTU discovery mechanism.

The third issue described in this advisory is the practicability of slowing the traffic between two hosts by sending ICMP Source Quench packets to an endpoint of the session. The technique used is to send a Source Quench packet including the details of the TCP connection to be targeted. According to RFC 1122, the Source Quench packet will limit the rate of the TCP connection.

It is possible to apply the TCP blind connection-reset vulnerability to ICMP Version 6 packets (the control protocol of IP Version 6) by equating hard errors to ICMPv6 Type 1 (Destination Unreachable) codes 1 (communication with destination administratively prohibited) and 4 (port unreachable). The Path MTU discovery attack could be affected by sending an ICMPv6 Type 2 code 0 ("Packet Too Big") packet, which does not describe a hard error but is used to determine end to end path MTU. Source quench is not defined in RFC 2463 for ICMPv6. Since IP Version 6 was not defined when RFC 1122 was written, the discussion in this advisory will concentrate on IP Version 4. Further details of how the attacks apply to

IP Version 6 is available in Fernando Gont's Internet Draft "ICMP attacks against TCP".

Details

532967/NISCC/ICMP/1

CVE number: [CAN-2004-0790](#)

RFC 1122 section 4.2.3.9 refers to some ICMP message types as representing hard errors. These message types are ICMP Type 3 (Destination Unreachable) codes 2 (Protocol Unreachable), 3 (Port Unreachable) and 4 (Fragmentation Needed and Don't Fragment was Set). For hard errors, according to RFC 1122 the TCP implementation should abort the connection. Thus by sending an ICMP Type 3, code 2, 3 or 4 with the IP header and the first 64 bits of the header of a TCP as its payload (the source and destination TCP ports and the sequence number), the receiving TCP implementation would reset the existing connection if it did not check that the sequence number was as expected.

It should be noted that the current RFCs do not recommend that TCP implementations check the sequence number. In section 5.1 of his Internet Draft "ICMP attacks against TCP" Fernando Gont states:

"TCP SHOULD check that the sequence number in the TCP header contained in the payload of the ICMP error message is within the range $SND.UNA \leq SEG.SEQ < SND.NXT$. This means that the sequence number should be within the range of the data already sent but not yet acknowledged. If an ICMP error message doesn't pass this check, it SHOULD be discarded." Here SND.UNA is the oldest unacknowledged sequence number, SEG.SEQ is the sequence number contained in the payload of the ICMP error message, and SND.NXT is the next sequence number to be sent. There is a dependency on the TCP window size as without scaling (see RFC 1323) the range of unacknowledged sequence numbers can be in the range SND.UNA to SND.NXT-1.

532967/NISCC/ICMP/2

CVE number: [CAN-2004-1060](#)

In the case where a host complies with RFC 1191 ("Path MTU Discovery"), it is possible to use the blind connection-reset attack with a ICMP Type 3 Code 4 packet and the addition of the "next-hop MTU" field in the ICMP header set to a value of 68 (octets) to slow down the transmission rate for traffic from the host.

532967/NISCC/ICMP/3

CVE number: [CAN-2004-0791](#)

RFC 1122 section 4.2.3.9 states "TCP MUST react to a Source Quench by slowing transmission on the connection. The RECOMMENDED procedure is for a Source Quench to trigger a "slow start," as if a retransmission timeout had occurred." Thus by sending an ICMP Type 4 (Source Quench) packet to a host with the IP header and the first 64 bits of the header of a TCP as its payload, the receiving TCP implementation would rate limit the existing connection if it did not check that the sequence number was expected. As noted above, the current RFCs do not recommend that TCP implementations check the sequence number.

Mitigation

The main impact of the TCP blind connection-reset vulnerability is on applications that are intolerant of loss of a TCP session, such as BGP. In this case applying an access control list to block ICMP Type 3 code 2, 3 and 4 packets to BGP routers will be an effective mitigation, as will the use of anti-spoofing measures in the case that the ICMP packet inducing the reset is sent from a spoofed IP address.

In the case of hosts which use Path MTU discovery, the only mitigation is to disable the use of the Path MTU discovery mechanism until the vendor provides a security patch.

The Source Quench vulnerability can be mitigated by applying an access control list blocking ICMP Type 4 packets on routers and by blocking ICMP Type 4 packets to corporate networks at the organisational boundary. Again, anti-spoofing measures such as URPF and access control lists blocking private, non-routable IP addresses at routers will also provide some protection if the source IP address of the ICMP packet is spoofed.

Solution

General solutions to the vulnerabilities are described in section 5 of Fernando Gont's Internet Draft "ICMP attacks against TCP" (see <http://www.ietf.org/internet-drafts/draft-gont-tcpm-icmp-attacks-05.txt>). These solutions include:

- Checking that the TCP sequence number is within the range of the data already sent but not yet acknowledged
- (On routers) checking that the TCP acknowledgement number is in the range of the last sequence number acknowledged to the next sequence number expected
- Randomising source (ephemeral client) port numbers (making the port number more difficult to guess)
- Providing authentication mechanisms for ICMP messages to ensure that an ICMP message is processed only if it is correctly authenticated
- Ingress and egress filtering on the IP addresses and TCP ports in the payload of ICMP packets
- Changing the behaviour of a TCP implementation when the ICMP message is not expected to cause a soft rather than a hard error
- Delaying the TCP connection reset until an ICMP error message indicating a hard error has been received a specified number of times
- To protect against resets against Path MTU Discovery, delay the handling of a ICMP Type 3 Code 4 ("packet too big" error)

packets in the case where the Path MTU has already been negotiated, i.e. where larger packets sizes have been already sent and acknowledged

- Changing the handling of ICMP hard error messages for connections in synchronized states to ignore the messages during the life of a connection or to treat them as soft errors
- Ignoring Source Quench ICMP packets

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

Credits

This issue was discovered by Fernando Gont (UTN/FRH) and is the subject of an Internet draft by the same author; "ICMP attacks against TCP" (see <http://www.ietf.org/internet-drafts/draft-gont-tcpm-icmp-attacks-05.txt>). The latest version of the Internet Draft can be obtained from <http://www.gont.com.ar/drafts/icmp-attacks-against-tcp.html>.

NISCC wishes to thank Fernando Gont for bringing this vulnerability to our attention and for agreeing to allow NISCC to co-ordinate the disclosure of this issue. NISCC also wishes to thanks Fernando for his comments on this advisory.

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/532967/index.html>.

[Alcatel](#)

[Apple](#)

[Check Point Software Technologies](#)

[Ltd](#)

[Cisco Systems](#)

[CyberGuard](#)

[Fedora Projects](#)

[Fujitsu](#)

[Hewlett-Packard](#)

[Hitachi](#)

[IBM](#)

[Juniper Networks](#)

[NEC](#)

[Nortel](#)

[Polycom Inc](#)

[Red Hat](#)

[Secure Computing Corporation](#)

[Stonesoft](#)

[Wind River](#)

[Alcatel](#)

In relation to this security advisory on a vulnerability in ICMP, Alcatel has conducted an immediate assessment to determine any impact this may have on its portfolio. A first analysis has shown that various Alcatel products can be affected, amongst others the A1000 E10, A1000 S12, 5020, 5430 SRB, 1300 NMC, 1357 LI, 7325, 7340 FTTU, 730x ASAM, 7670, 5620, 59xx and mobile products. We will take appropriate actions when required, together with our third party software providers, to limit the risks implied by this vulnerability. Customers may contact their Alcatel support representative for more details. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential security vulnerabilities.

Apple

Apple: The ICMP issue described in this advisory does not affect:

- Mac OS X v10.2 or later versions
- Mac OS X Server v10.2 or later versions

Check Point Software Technologies Ltd

Check Point products are not vulnerable to this issue.

Cisco Systems

Please visit the following link for Cisco's advisory:

<http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>

CyberGuard

CyberGuard's Quality Assurance testing has confirmed that both the Classic 5.2.1 and TSP 6.1 security appliance families are not susceptible to the NISCC reported vulnerability "/icmp/532967." Risks are mitigated by inclusion of multiple embedded technologies, including source port randomization, anti-spoofing protection and granular packet filter control of ICMP types/codes.

CyberGuard's Security Alert Team is continuously subjecting our products to industry reported attacks, and takes the added precaution of performing vulnerability variant testing. These tests, and ongoing product enhancements, ideally position CyberGuard to mitigate current and emerging security threats.

Fedora Project

CAN-2004-0790: A blind TCP connection reset by sending

The Linux 2.4 and 2.6 kernels have always verified the TCP sequence number on ICMP errors. In addition Linux kernels will never abort a connection due to a received ICMP packet. All Fedora Core versions are therefore unaffected by this issue.

CAN-2004-0791: A spoofing attack with ICMP type 4 header

The Linux kernel since 2.6.9 and 2.4.28 has included a patch by Dave Miller to ignore ICMP Source Quench messages as recommended by Fernando Gont. Fedora Core 3 shipped with a 2.6.9 kernel which ignores ICMP Source Quench messages. Fedora Core 2 was updated to a 2.6.9 kernel in a November 2004 update and is therefore also unaffected by this issue.

CAN-2004-1060: ICMP path MTU spoofing

Linux 2.4 and 2.6 kernels verify the sequence number on ICMP errors, thus significantly mitigating this issue. This issue can also be mitigated by disabling PMTU discovery if not required (/proc/sys/net/ipv4/ip_no_pmtu_disc).

Fujitsu

Status received on April 13th 2005:

Information for this issue is available:

<http://software.fujitsu.com/jp/security/niscc/niscc.html#222750-tcpicmp>

IBM

The AIX Operating System is affected by the issues discussed in NISCC vulnerability #532967 and CERT Vulnerability note VU#222750. An advisory for this issue will be available via

<https://techsupport.services.ibm.com/server/pseries.subscriptionSvc>

IBM eServer Platform Response:

For information related to this and other published Advisories that may relate to the IBM eServer Platforms (xSeries, iSeries, pSeries, and zSeries), please go to

<https://app-06.www.ibm.com/servers/resourcelink/lib03020.nsf/pages/securityalerts?OpenDocument&pathID=>

In order to access this information you will require a Resource Link ID. To subscribe to Resource Link go to <http://app-06.www.ibm.com/servers/resourcelink> and follow the steps for registration.

All questions should be referred to servsec@us.ibm.com.

Hewlett-Packard

HEWLETT-PACKARD COMPANY SECURITY BULLETIN: HPSBUX01164
Originally issued: 25 May 2005
Reference ID: NISCC #532957, SSRT4884

HP has published Security Bulletin HPSBUX01164 with solutions for HP-UX B.11.00, B.11.04, B.11.11, B.11.22, and B.11.23.

HEWLETT-PACKARD COMPANY SECURITY BULLETIN: HPSBTU01210
Originally issued: 15 July 2005
Reference ID: NISCC #532957, SSRT4743, SSRT4884

HP has published Security Bulletin HPSBTU01210 with solutions for HP Tru64 UNIX 5.1B-3, 5.1B-2/PK4, 5.1A PK, 4.0G PK4, and 4.0F PK8.

These bulletins are available from the HP IT Resource Centre page at: <http://itrc.hp.com> "Maintenance and Support" then "Support Information Digests" and then "hp security bulletins archive" search for bulletin HPSBUX01164 or HPSBTU01210.

To report potential security vulnerabilities in HP software, send an E-mail message to: security-alert@hp.com

Hitachi

[VULNERABLE]

Hitachi GR2000/GR4000/GS4000/GS3000 is vulnerable to this issue.

More details are available at

<http://www.hitachi.co.jp/Prod/comp/network/notice/NISCC-532967.html>

(Japanese)

[NOT VULNERABLE]

Alaxala AX series are NOT vulnerable.

Juniper Networks

Juniper Networks M-series and T-series routers running certain releases of JUNOS software are susceptible to this vulnerability.

Other Juniper Networks products are not susceptible to this vulnerability. Customers should visit the Juniper Networks Customer Service Centre web-site for further information.

<https://www.juniper.net/customers/csc>

NEC

NEC Corporation products are not susceptible to this vulnerability.

- We continue to check our products.
- For more detail:

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

Nortel

Nortel has posted several bulletins on this issue at our Technical Support site; the URL is

<http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=SECUREADVISORY#>

Polycom Inc

Polycom has investigated the potential impact to our products for NISCC Advisory 532967. Specific product information will be provided at <http://www.polycom.com/securitycenter>.

Red Hat

CAN-2004-0790: A blind TCP connection reset

Red Hat Enterprise Linux 2.1 and 3 kernels have always verified the TCP sequence number on ICMP errors. In addition Linux kernels will never abort a connection due to a received ICMP packet. All Red Hat Enterprise Linux versions are therefore unaffected by this issue.

CAN-2004-0791: A spoofing attack with ICMP type 4 header

Red Hat Enterprise Linux 2.1 and 3 kernels prior to January 2005 honour ICMP Source Quench messages, although the TCP sequence number is checked which substantially increases the amount of effort an attacker would need to be able to cause a successful attack. ICMP Source Quench messages were disabled completely by the following updates:

<http://rhn.redhat.com/errata/RHSA-2005-043.html>

<http://rhn.redhat.com/errata/RHSA-2005-016.html>

<http://rhn.redhat.com/errata/RHSA-2005-017.html>

CAN-2004-1060: ICMP path MTU spoofing

Red Hat Enterprise Linux 2.1 and 3 kernels verify the sequence number on ICMP errors, thus significantly mitigating this issue. This issue can also be mitigated by disabling pmtu discovery if not required (/proc/sys/net/ipv4/ip_no_pmtu_disc).

Secure Computing Corporation

Secure Computing has carefully analyzed the scenarios outlined in the Internet Draft, and has determined that the Sidewinder G2 responds appropriately in those situations. Some of the scenarios mentioned in this draft illustrate again the desirability of using carefully configured security appliances and using protocols such as IPSec.

Stonesoft

Stonesoft StoneGate Firewall and IPS products are not affected by these vulnerabilities.

Wind River

Response and Plan for TCP Internet-Draft Documents

Jan Provan
2/11/05

Introduction

Two Internet-Draft documents were submitted at the August 2004 IETF meeting. They have subsequently been updated and submitted to both CERT and NISCC as TCP vulnerabilities. They both identify potential areas where TCP is vulnerable to a DoS attack. This statement describes Wind River stack's implementation and exposure to these issues. Where appropriate a plan for relief is described.

The drafts are:

<http://www.ietf.org/internet-drafts/draft-gont-tcpm-tcp-soft-errors-01.txt>
<http://ietfreport.isoc.org/idref/draft-gont-tcpm-icmp-attacks/>

All of these attacks assume the TCP four-tuple is known. Given that initial requirement these attacks are not considered high risk.

These documents have been submitted to both CERT and NISCC as TCP vulnerabilities. The CERT vulnerability number is: #222750 and the NISCC number is: #532967. Both organizations plan to release the vulnerabilities sometime in early 2005. Pre-alerts have been sent out to members of these two organizations.

TCP's Reaction to Soft Errors

Upon analysis of this draft, Wind River does not plan on taking any action. The default timeout for TCP connection setup in the Wind River stack is 75 seconds.

In all releases after VxWorks 5.3 a hard error does not result in TCP aborting the connection. The hard error code is saved by TCP. If the connection is dropped due to a timeout this error code is available to the application. It is up to the applications to react to the error.

The stack released with VxWorks 5.3 and before is a bit more vulnerable to hard errors in that it sends the error to the application immediately. If the application chooses to close the connection immediately then the attack is successful.

TCP ICMP Attacks

Blind Connection Resets – This attack assumes the stack aborts a connection on a hard error. The current Wind River Network Stacks

do not handle hard errors in that way so are not vulnerable to this attack. A hard error will not abort the connection through TCP. The behavior of various releases of the stack concerning hard errors is described above.

Source Quench – The legacy Wind River stacks are vulnerable to this attack in that the performance will degrade. The connection is not reset. Another potential point of degradation is the ICMP “needs fragmentation” message. The proposed solution of checking the TCP sequence number in the data portion of the ICMP message will address both possibilities.

Wind River will provide patches where the TCP sequence number is checked for the 5.5.x and 5.4 releases by April 2005. No earlier releases will be patched.

The dual Ipv4/Ipv6 stack already checks the sequence number. This stack is available with all the platforms and VxWorks 6.0.

Summary

Wind River does not believe these potential attacks warrant an immediate emergency response. They are viewed as a medium risk and will be addressed in the normal course of maintenance releases.

Wind River will track these two drafts through the IETF and monitor updates and comments.

Wind River Network Stack 2.0 already checks the ICMP sequence numbers. The release of VxWorks 6.0 and the MSP updates shipping in the fall of 2004 are based on this stack.

Wind River is planning updates to the 5.5 and 5.4 versions of the stack. These updates will be released by April 2005.

Contact Information

The NISCC Vulnerability Management Team can be contacted as follows:

Email	vulteam@niscc.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

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.

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

12 April 2005	Initial Release (1.0)
	Amended IBM's vendor statement (1.1)
14 April 2005	Added Alcatel's vendor statement (1.2)
18 April 2005	Added Nortel's vendor statement (1.3)
	Amended Fujitsu's vendor statement (1.4)
27 April 2005	Added HP's vendor statement (1.5)

19 May 2005 Updated Hitachi's vendor statement (1.6)
31 August 2005 Updated HP's vendor statement (1.7)
6 December 2005 Updated link to Internet Draft (1.8)

<End of NISCC Vulnerability Advisory>