

National Infrastructure Security Co-ordination Centre

NISCC Vulnerability Advisory 006489/OpenSSL2

Vulnerability Issue in OpenSSL

Version Information

Advisory Reference	006489/OpenSSL2
Release Date	4 November 2003
Last Revision	8 December 2003
Version Number	1.1

What is Affected?

OpenSSL 0.9.6k on Microsoft Windows. Version 0.9.7 is not affected.

Severity

Denial of Service

Summary

During 2002 the University of Oulu Security Programming Group (OUSPG) discovered a number of implementation specific vulnerabilities in the Simple Network Management Protocol (SNMP). NISCC has performed and commissioned further work to identify implementation specific vulnerabilities in related protocols that are vital to the UK Critical National Infrastructure (CNI). The OpenSSL implementation of the TLS (Transport Layer Security) and SSL (Secure Sockets Layer) protocols, which add communications protection to a range of Internet protocols, has been studied in this context.

NISCC has provided a test suite to the OpenSSL project. The OpenSSL development team has utilised the test suite to determine whether their product is vulnerable.

New versions of OpenSSL were released on [30 September](#) to address the issues discovered. Subsequent to this release [Novell Inc.](#) carried out further testing using the NISCC suite. They discovered that there was an additional denial of service vulnerability in OpenSSL version 0.9.6k when running on a Windows platform.

Dr Stephen Henson of the OpenSSL core team researched the report and created a patch for the vulnerability identified.

Details

OpenSSL is an open source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a general purpose cryptography library.

The vulnerabilities described in this advisory affect the OpenSSL implementation of the TLS and SSL protocols, which are typically used to provide security services to a range of Internet application protocols and in support of web and email applications.

TLS and SSL are intermediate protocols layered onto a TCP connection used to provide additional security to higher level protocols. These higher level protocols, particularly application protocols such as web services or email, may be layered on top of a TLS/SSL connection.

TLS is based on SSL v3, and although the two are not interoperable, implementations of TLS v1 are likely to support SSL v3. For the purpose of this discussion the two will be considered equivalent. TLS and SSL are not Abstract Syntax Notation One (ASN.1) based protocols and define their own presentation language as part of the TLS/SSL specification. However, they do depend on a number of ASN.1 objects used as part of the protocol exchange.

A bug in OpenSSL 0.9.6 would cause certain ASN.1 sequences to trigger a large recursion. On platforms such as Windows this large recursion cannot be handled correctly and so the bug causes OpenSSL to crash. A remote attacker could exploit this flaw by sending a client certificate to an accepting server which would cause a denial of service. We do not believe this issue could be exploited further.

Vendor specific information will be released as it becomes available and if vendor permission has been received. Subscribers are advised to check the following URL regularly for updates:

<http://www.uniras.gov.uk/vuls/2003/006489/openssl2.htm>

[Please note that updates to this advisory will not be notified by email.]

NISCC are tracking this vulnerability as NISCC/006489/OpenSSL2/1

The CVE identifier CAN-2003-0851 has been allocated, details of which can be found at <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0851>

Solution

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

A patch has been released by the OpenSSL core team that addresses this issue.

The OpenSSL advisory is available from:
http://www.openssl.org/news/secadv_20031104.txt

The patch is available from the OpenSSL site at

<http://www.openssl.org/source>

or from the NISCC web site at:

<http://www.uniras.gov.uk/vuls/2003/006489/openssl2patch.asc>

[This vulnerability was discovered by [Novell Inc.](#), utilising the NISCC TLS/SSL test suite. Stephen Henson, a member of the OpenSSL Core Team (steve@openssl.org), developed the patch.]

Vendor Information

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

Hitachi

Hitachi products are not affected by this issue.

Nortel

The following Nortel Networks Generally Available products are potentially affected by the vulnerabilities identified in NISCC Vulnerability Advisory 006489/OpenSSL2:

Periphonics:
PERIhtmls version 2.0.0 is potentially affected; patch htmls2.0.0.7 is available. For more information on obtaining and installing the patch please contact Nortel Networks.

Optivity Products:
Optivity Policy Services versions 3.1 and 3.1.1 are potentially affected; a patched release of each version is available. For more information on obtaining and installing the patched release please contact Nortel Networks.
Optivity NetID is currently under review; this Vendor Statement will be updated as soon as NetID's status has been determined.

For more information please contact
North America: 1-800-4NORTEL or 1-800-466-7835
Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009

Contacts for other regions are available at
<<http://www.nortelnetworks.com/help/contact/global/>>

Or visit the eService portal at <<http://www.nortelnetworks.com/cs>> under Advanced Search.

If you are a channel partner, more information can be found under <<http://www.nortelnetworks.com/pic>> under Advanced Search.

Red Hat, Inc.

This vulnerability does not affect the versions of OpenSSL as shipped or updated in any Red Hat product.

Contact Information

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)20 7821 1330 Extension 4511 <i>(Monday to Friday 08:30 - 17:00)</i>
Fax	+44 (0)20 7821 1686
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/UNIRAS.asc>.

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@nisc.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.nisc.gov.uk/aboutnisc/index.htm>

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.

© 2003 Crown Copyright

Revision History

November 4, 2003: Initial release
December 8, 2003: Vendor statement from Hitachi

<End of NISCC Vulnerability Advisory>