

## **NISCC Vulnerability Advisory 729618/NISCC/PARASITIC-KEYS**

### **Denial-of-Service Condition Affecting X.509 Certificates Verification**

#### **Version Information**

Advisory Reference	729618/NISCC/PARASITIC-KEYS
Release Date	28 September 2006
Last Revision	03 October 2006
Version Number	1.2

#### **Acknowledgement**

This vulnerability was reported to NISCC by Dr Stephen N. Henson.

#### **What is Affected?**

In general, any implementations that will perform some sort of certificate verification may be affected.

Please note that the information contained within this advisory is subject to changes. All subscribers are therefore advised to regularly check the NISCC website (<http://www.niscc.gov.uk/niscc/vulnAdv-en.html>) for updates to this notice.

#### **Impact**

If exploited, this vulnerability can potentially lead to a denial-of-service (DoS) condition.

#### **Severity**

The severity of this vulnerability varies by vendor. Please see the 'Vendor Information' section below for further information. Alternatively, contact your vendor for product specific information.

#### **Summary**

X.509 is a widely used ITU-T standard for defining digital

certificates. X.509 certificates carry public keys which are used for a variety of purposes including digital signature verification.

However some applications that perform certificate verification may be subjected to a denial-of-service condition if certain malicious keys (referred to as Parasitic Keys in this advisory) are used.

Please note that the information contained within this advisory is subject to changes. All subscribers are therefore advised to regularly check the NISCC website (<http://www.niscc.gov.uk/niscc/vulnAdv-en.html>) for updates to this notice.

## **Details**

Signature verification can be rapidly processed by the RSA algorithm by choosing appropriate public key components. The main RSA verification operation is to calculate  $S^e \pmod n$ , where:

- S is the signature
- e is the public exponent
- n is the public modulus

The public exponent is typically a small value (i.e. typically 3, 5 or 65537) and the value of n is 1024 or 2048 bits in size. The small value of e reduces the amount of processing required to verify a signature.

However by choosing much larger values for e and n, it may be possible to cause the verification process to consume large amounts of system resources and hence result in a denial-of-service condition.

Please note that by restricting the size of the public exponent will still allow for large key sizes to be used.

## **Mitigation**

Please see the 'Vendor Information' section for recommendations on possible mitigation methods.

## **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](#) 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-729618/index.html>

Barron McCann

Intoto Inc

Mozilla

OpenSSL

Tumbleweed Communication Corp

Barron McCann

Following the recent NISCC advisory regarding a potential denial of service attack caused by the use of x509 certificates, we would like our customers to know that all current products in the X-Kryptor range are unaffected by this vulnerability.

We have prepared a statement which is available on our website.

<http://www.bemac.com/ISec/s2pressrelease.asp?PRID=136&S2ID=14>

Intoto Inc

Intoto engineering team investigated potential vulnerability of Parasitic Public Keys documented in this NISCC advisory, and found that its' VPN and SSLVPN products are affected. Intoto has produced patch for this vulnerability. Please contact Intoto at [support@intoto.com](mailto:support@intoto.com) to get this patch.

Mozilla

The Mozilla NSS library limits the length of the modulus and exponent to prevent denial of service attacks. The default limits of 8192 bits for the modulus and 64 bits for the exponent were chosen considering typical uses and hardware and could be adjusted for custom applications, such as installations on a low-powered embedded device.

OpenSSL

The CVE numbers CVE-2006-2937 and CVE-2006-2940 were assigned to issues in OpenSSL related to this research. Please refer to the following link for a vendor statement and details of patches for OpenSSL:

[http://www.openssl.org/news/secadv\\_20060928.txt](http://www.openssl.org/news/secadv_20060928.txt)

Tumbleweed Communication Corp

Tumbleweed has evaluated these test cases and determined that our products are not vulnerable to the parasitic keys included with the test cases. Our products' code that processes certificates and keys treated these non-standard certificates with parasitic keys as invalid and refused to accept them for use in any cryptographic processes.

## Acknowledgements

The NISCC Vulnerability Management Team would like to thank Dr Stephen N. Henson for his effort in researching this issue, reporting it to NISCC and for his assistance in the handling of this vulnerability.

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

## Contact Information

The NISCC Vulnerability Management Team can be contacted as follows:

Email	<a href="mailto:vulteam@nisc.gov.uk">vulteam@nisc.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.nisc.gov.uk/nisc/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@nisc.gov.uk](mailto: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.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.

© 2006 Crown Copyright

### **Revision History**

28 September 2006	Initial release (1.0)
28 September 2006	Updated document with CVE numbers for OpenSSL (1.1)
03 October 2006	Added statement from Barron McCann (1.2)

<End of NISCC Vulnerability Advisory>