RSA Security Bulletin

Subject: Security Patch Released for RSA BSAFE SSL-C
Posted: August 2002

Dear RSA Security Customer:

On July 30, 2002, the CERT Coordination Center announced multiple vulnerabilities in OpenSSL. During the past week, RSA has investigated whether these vulnerabilities also impact RSA BSAFE SSL products. We have determined that SSL-C is impacted by a subset of these vulnerabilities.

This bulletin highlights the impact of these vulnerabilities on our SSL products. In addition, this advisory outlines the process that customers should follow to request patch downloads.

Security Issue
The CERT Coordination Center announced five vulnerabilities that impact OpenSSL and SSLeay. Four of these vulnerabilities are related to buffer overflows and the final vulnerability is caused by ASN.1 encoding issues.

In reviewing the RSA BSAFE SSL code, we have determined that:

- SSL-J and SSL-C ME are not impacted by these vulnerabilities.

- SSL-C is impacted by three of the five vulnerabilities that affected OpenSSL. In particular:

    - SSL-C is impacted by the buffer overflows caused by the use of a malformed client key during the SSL v2 handshake process (referred to as CAN-2002-0656). This is **only** a security concern if SSL v2 is enabled. SSL v2 is an older protocol with other known security vulnerabilities. The majority of currently deployed applications only support SSL v3 and TLS v1 and do not support SSL v2.

    - SSL-C is affected by the buffer overflows in the ASCII representations of integers on 64-bit platforms (referred to as CAN-2002-0655). This vulnerability **only** applies when a 64-bit application runs on a 64-bit platform. Note that 32-bit applications running on 64-bit platforms are not impacted by this vulnerability.

    - SSL-C is impacted by the ASN.1 library vulnerability (referred to as CAN-2002-0659). This vulnerability occurs because the ASN.1 engine used by SSL-C incorrectly parses malformed certificate data. An SSL client is exposed to this vulnerability because it needs to parse data from a server. However, an SSL server is **only** exposed to this vulnerability if client side authentication is enabled. Most applications do not use client side authentication, and are not impacted by this vulnerability.

RSA Security is unaware of any security breach resulting from these vulnerabilities.

RSA Recommendation
RSA Security recommends that all RSA BSAFE SSL customers review this bulletin to determine if they are impacted by these vulnerabilities and, if so, register for a download of security patches immediately to minimize their security risks.

Solution
We currently have patched versions of SSL-C 2.1, 2.2, and 2.3 available for download. In addition, RSA will continue to release patches for other SSL-C versions as these are completed. For target dates on patch availability, please refer to: http://www.rsasecurity.com/sslsecurityupdates

Our updated products are available for both binary and source customers. The binary releases have been tested on multiple platforms so that customers can ensure that the update will indeed work on their required platforms.

In the addition, our patches prevent potential denial of service attacks. During an attempted exploit of these security vulnerabilities, RSA updated products will return an error condition to the caller so that applications can take whatever action is deemed appropriate rather than simply abort the application.

Patch Registration
To ensure that our customers are informed about the most recently available patches and to expedite patch download, RSA has created a patch update page and download registration form that can be accessed at:
http://www.rsasecurity.com/sslsecurityupdates

RSA Security encourages customers to install patches to proactively prevent security problems. RSA Security continues to make all possible efforts to ensure our products meet the quality and standards our customers expect.

If you have a current support contract, please contact support for assistance. Support is available worldwide and local support contact information is available at: http://www.rsasecurity.com/support/contact.html

If you do not have a current support contract, you will need to contact your local sales representative.