

[UNIX] Buffer Over/Underflows Found in SSLdump

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0042.html>

From: support@securiteam.com

Date: 09/12/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 12 Sep 2002 08:45:45 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Buffer Over/Underflows Found in SSLdump

SUMMARY

It is possible to send <<http://www.rtfm.com/ssldump>> ssldump bogus protocol messages that will cause a buffer under/overflow. Although no exploit is known, it is possible that this buffer overflow can be used to take control of ssldump, which might lead to execution of arbitrary code and compromise of the affected system.

DETAILS

Vulnerable systems:

- * Any version of ssldump prior to ssldump-0.9b3

There are two problems:

(1) ssldump attempts to decrypt the PreMasterSecret into a 48 byte buffer. This is the longest legal value for an RSA PreMasterSecret. It's possible to overflow this buffer by using a longer PMS. The maximum size of this overflow is limited by the length of the server's RSA key and therefore will be about 64-bytes for a 1024-bit RSA key. This bug can only be exercised in decryption mode.

(2) ssldump does not check the length of an SSLv2 "challenge" value. The challenge value is copied into a right-aligned 32-byte buffer and therefore it is possible to underrun the buffer by up to 64k.

Securiteam: [UNIX] Buffer Over/Underflows Found in SSLdump

Scope of vulnerability:

Since ssl dump is an analysis tool, you have to be actually running it at the time when an attacker attempts to attack you. However, this is not impossible. If you are running ssl dump on a network where hostile parties can send you traffic, you should stop or upgrade.

Fix:

Upgrade to ssl dump-0.9b3, found at:

<http://www.rtfm.com/ssl dump/ssl dump-0.9b3.tar.gz>

<http://www.rtfm.com/ssl dump/ssl dump-0.9b3.tar.gz>

ADDITIONAL INFORMATION

The information has been provided by <mailto:ekr@rtfm.com> Eric Rescorla.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[TOOL] SSLDump a SSLv3/TLS Network Protocol Analyzer"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)