

Transport Layer Security (TLS) handshake renegotiation weak security CVE-2009-3555

Problem Description

All customers using Communications Server for Linux on System z TN3270 Server relying on Secure Socket Layer v3 (SSLv3) or any of the multiple versions of Transport Layer Security (TLS) in support of secure communications between a client and server or between server and server are impacted by a recently discovered weakness in the TLS and SSL v3 protocols. SSLv2 is not affected.

The TLS/SSL weakness exists in multiple implementations of the Transport Layer Security (TLS) protocol, including SSL.

To address the weakness in the TLS/SSL handshake renegotiation, IBM, along with the other members in the Industry Consortium for the Advancement of Security on the Internet (ICASI), are working together with the Internet Engineering Task Force (IETF) to enhance and strengthen the handshake renegotiation protocol in the TLS specification. This effort will take some time to complete. The delivery outlook for inclusion of this enhanced handshake renegotiation capability in TLS protocol implementations is unknown at this time.

In the interim, Communications Server for Linux on System z support is delivering a fix to allow an installation to disable the TLS handshake renegotiation. The TLS handshake renegotiation is rarely used. Disabling the TLS handshake renegotiation will block a remote attacker from attempting to exploit the weakness in the TLS protocol. After installing this fix, the default setting will disable the TLS handshake renegotiation. The fix also provides the user with an option to re-enable renegotiation if warranted. TLS handshake renegotiation should be re-enabled only if absolutely necessary and with a clear understanding and acceptance of the potential security risks.

Communications Server for Linux on System z:

The CS Linux on System z V6.4.0.2, APAR LI75612, enables the GSKIT V7.0.4.27 to optionally override new default of disabling TLS handshake renegotiations. After installing CS Linux on System z V6.4.0.2 and “gskbas-7.0.4.27” on the System z Linux image, you can override the new default by setting environment variable, **GSKIT_RENEGOTIATION**, before the Communications Server product starts (“sna start” is executed). The options are **NONE** (default), **ABBREVIATED**, **FULL**. To optionally override the default, follow these instructions:

INSTRUCTIONS:

Included in this APAR is a file, "environment", which has the options documented. Edit the file to select the option if the default needs to be overridden. Place the file in the following path: /etc/opt/ibm/sna/environment

Contents of "environment" file:

```
#
# The environment variable GSKIT_RENEGOTIATION is used to override
# the default behavior for TLS/SSL handshake renegotiation.
# TLS handshake renegotiation should be re-enabled only if absolutely
# necessary and with a clear understanding and acceptance of the
# potential security risks.
#
# There are 3 settings: NONE, ABBREVIATED, FULL
# The default is NONE.
# The environment variable is: GSKIT_RENEGOTIATION
# The following will set the behavior to allow full renegotiations:
#
# export GSKIT_RENEGOTIATION=FULL
#
```