Impact of POODLE (CVE-2014-3566) on z/VSE

POODLE stands for Padding Oracle On Downgraded Legacy Encryption. This vulnerability allows a man-in-the-middle attacker to decrypt cipher text using a padding oracle side-channel attack. More details are available in the upstream OpenSSL advisory. POODLE affects older standards of encryption, specifically Secure Socket Layer (SSL) version 3. It does not affect the newer encryption mechanism known as Transport Layer Security (TLS).

As POODLE discovered a vulnerability in the SSL 3.0 protocol version, this is not a bug in any given SSL implementation, but an issue of the specification itself. As a consequence, there is no bug fix for any SSL implementation. Instead it is recommended that z/VSE applications should no longer use SSL 3.0. You may consult the z/VSE documentation for configuration options of z/VSE components and applications to avoid SSL 3.0.

You can find more information on these web sites:

- National Vulnerability Database (NVD)
- Vulnerability Summary for CVE-2014-3566
- Paper: This POODLE Bites: Exploiting the SSL 3.0 Fallback (pdf document)
- Redhat information: POODLE: SSLv3 vulnerability (CVE-2014-3566)
- Configuring SSL for CICS Web Support and MQ (IBM Redbook: Security on IBM z/VSE)
- Security Bulletin: Vulnerability in SSLv3 affects IBM WebSphere MQ, IBM WebSphere MQ Internet Pass-Thru and IBM Mobile Messaging and M2M Client Pack (CVE-2014-3566)
- Security Bulletin: POODLE vulnerability in SSLv3 affects IBM Explorer for z/OS and IBM CICS Explorer (CVE-2014-3566)
- Security Bulletin: POODLE vulnerability in SSLv3 affects IBM CICS Transaction Gateway (CVE-2014-3566)
- z/VSE documentation (z/VSE Administration, z/VSE e-business Connectors, User’s Guide, z/VSE TCP/IP Support, TCP/IP for VSE Installation / User's Guide, IPv6/VSE SSL Installation, Programming and User's Guide)

New APAR for CICS TS for VSE/ESA 1.1.1

APAR PI28366 / PTF UI23574 causes CICS TS to use the TLS 1.0 protocol for SSL connections as the minimum protocol level required, but it also introduces a new option for the DFHSIT macro to allow the SSLV3 protocol to be used.

SSL version 3.0 should only be used for a migration period while clients that still require this protocol are upgraded.

DFHSIT macro parameter:

> ENCRYPTION={WEAK|NORMAL|STRONG|**SSLV3**}
>
> SSLV3 allows the use of TLS version 1.0 and SSL version 3.0. If any of the clients that connect do not support TLS 1.0, you can select SSLV3. CICS TS will then accept less secure SSL V3 client connections. SSLV3 implies the use of the STRONG encryption cipher suites.

Please consult the CICS TS for VSE/ESA Enhancements Guide for more details on the DFHSIT macro parameters.