Customer Actions: POODLE SSLv3

October 21, 2014

All browsers and released versions of Niagara may be affected.

Acting on **Alert TA-14-290A** from the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), Tridium has identified fixes and guidance for customers regarding the SSLv3 protocol. For Niagara users, this vulnerability can enable an attacker to hijack an encrypted session between a client and a server that supports SSLv3.

Issue

This vulnerability (CVE-2014-3566), commonly referred to as POODLE (Padding Oracle on Downgraded Legacy Encryption), allows the potential for a man-in-the-middle attacker to decrypt ciphertext using a padding oracle side channel attack. This affects Secure Sockets Layer (SSL) version 3 but does not affect the newer encryption mechanism known as Transport Layer Security (TLS).

All Niagara installations currently have the SSLv3 protocol as an option, including:

- JACE 2, 4, and 5 devices running any Niagara release, and all other systems using Niagara AX 3.6 and earlier.
- JACE 3, 6, and 7 devices, and all other systems using Niagara AX 3.7 and 3.8.

Customer Actions

- **For JACE 3, 6, and 7 devices**, and for all other systems using Niagara AX 3.7 and 3.8, remove SSLv3 as an option on the Web Service, FoxService, and Niagarad (Platform Information) screens and set the protocol to TLSv1.

  Download *Diagrams and Instructions*.

- **For JACE 2, 4, and 5 devices running any Niagara release, and for all other systems using Niagara AX 3.6 and earlier**, set a restriction in the web browser to support TLSv1 or higher.

For More Information

As we continue to research this issue, we will provide updates as they are available. If you have any questions, please feel free to contact your Tridium sales representative directly, or email our Sales Support team at support@tridium.com.