Security Risk Report

The OpenSSL team has published vulnerabilities through its mailing channels on April 09, 2014. See https://www.openssl.org/news/vulnerabilities.html for complete list.

Because the OPC UA ANSI C Stack can optionally use OpenSSL for TLS/SSL encryption, the Unified Automation Security Response Team has validated the reported vulnerables and strongly recommends to update your OpenSSL libraries.

The following updates to OpenSSL were released:

1.0.1g

OpenSSL has a serious vulnerability, called the “Heartbleed Bug” . Whether you are affected or not depends on the version and configuration of the OPC UA SDK and the OpenSSL version that are used. The latest Windows versions of our SDKs were shipped with OpenSSL 1.0.1f for convenience reason, The OpenSSL 1.0.1.f is affected by this bug. However, OPC UA is only affected if the new HTTPS based OPC UA protocol is used (by default it is disabled in our SDKs).

Affected Products/Versions:

- **C++ based OPC UA SDK V1.4.0** (Windows)
- **ANSI C based OPC UA SDK V1.4.0** (Windows)

Important: You are only affected if you have enabled the optional HTTPS protocol in your product configuration! HTTPS endpoints are disabled by default. The HTTPS protocol is experimental, not completely tested and not officially supported by Unified Automation.

Affected OpenSSL Versions:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

Recommendation:

- If your OPC UA server has **disabled HTTPS** (default), there is nothing to do.
- If your OPC UA server has **enabled HTTPS**
  - disable it if it is not needed
  - **On Windows:** Download OpenSSL 1.0.1g from http://www.openssl.org and recompile your SDK and server with that version.
  - **On Linux/Solaris:** Use your package manager to update the system’s OpenSSL library. Our SDKs are using the system’s library by default.
  - **On embedded systems:** Update the OpenSSL version of your cross-compiling toolchain and recompile your SDK and server.

FAQ:

- **Are older SDKs affected?** No, because they didn't include the HTTPS support.
- **Are .NET based SDKs affected?** No.
- **Are JAVA based SDKs affected?** No.
- **Are Clients affected?** Yes, if they use the C++ based SDK V1.4.0 SDK with HTTPS enabled.
- **Is UaExpert affected?** No. The latest release does’t include the HTTPS protocol.