Security Risk Report

The OPC Foundation has published CVE-2022-44725 through a security bulletin on November 17, 2022. See https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-44725 for details.

This vulnerability is caused by a feature in OpenSSL, which automatically loads a configuration file from given default location when being initialized. The default directory is set to a protected location in the file system (i.e. on Linux: `/usr/local/ssl`, on Windows: `C:\\Program Files\Common Files\\SSL`). However, when building the OpenSSL library from source, the OPENSSLDIR may accidentally be set to a path outside protected file system location. An unprivileged user can create subdirectories and lead to a specially-crafted openssl.cnf file to achieve arbitrary code execution with high privilege-user. The OPC Foundation public deliverable LDS (Local Discovery Server) is setting the path to hardcoded path (C:\Build\Projects\UA-LDS\stack\openssl\ssl).

Rating:

The vulnerability is rated with a Base Score of 7.8 and a Temporal Score of 7.0 according to the CVSS v3.1 metric with the following vector:

AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Details regarding prevention:

The vulnerability only affects users of OpenSSL that have set the OPENSSLDIR to a distinct location, hence not using the default file location. As a workaround administrators can create the subdirectories and set file system permissions to block this vulnerability. In addition OpenSSL (since v1.1.0) can be build with compiler option no-autoload-config, thereby prevented from loading any configuration file whatsoever.

Affected Products/Versions:

OpenSSL (third-party) is not part of the Unified Automation SDK delivery, except for evaluation editions and examples. Customers are responsible for choosing the latest OpenSSL version and building OpenSSL with correct parameter set including correct OPENSSLDIR. The OPC Foundation's LDS is not part of the Unified Automation SDK delivery and is not part of any Runtime Product delivery of Unified Automation.

> Important: If you are using OPC Foundation's LDS components, you should immediately update to the latest version (v1.04.405.479). Generally when using OpenSSL, you should check for correct OPENSSLDIR set to a protected location (admin rights required).

Recommendation:

- If your application uses Unified Automation C++ based OPC UA SDK, or AnsiC based OPC UA SDK, or High Performance SDK in combination with any OpenSSL version, you should immediately check your build environment regarding the correct OPENSSLDIR path.
- If you use the UaExpert and/or UaGateway the shipped OpenSSL has default path set as intended, hence components are not considered vulnerable.

FAQ:

- **Is the .NET based OPC UA Client Server SDK affected?** No, the .NET SDK does not use OpenSSL crypto library directly. However, many .NET SDK customers use the "certificategenerator.exe", which internally uses OpenSSL for initially creating application instance certificate. We strongly recommend using the "certificategenerator.exe" created by Unified Automation (do not use OPC Foundation's certificategenerator.exe)