Security Risk Report

The OpenSSL Software Foundation has published CVE-2022-0778 through a security bulletin on March 15, 2022. See https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778 for details.

This vulnerability is caused by a bug in the modular square root function in OpenSSL. This function is used when parsing certificates that contain elliptic curve public keys in compressed form. Even though our OPC UA products do not use ECC, any operation which requires the public key from the certificate will trigger the infinite loop by a specially crafted certificate. Parsing the certificate is performed before it's validation, parsing certificate is done on Client and on Server side, hence this vulnerability is rated Denial of Service (DoS). All our Unified Automation C++ and C based OPC UA SDKs, client and server side, using OpenSSL are affected, furthermore our Unified Automation runtime products UaExpert and UaGateway are affected.

Rating:

The vulnerability is rated with a Base Score of 7.5 and a Temporal Score of 6.7 according to the CVSS v3.1 metric with the following vector:

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

Details regarding prevention:

The vulnerability only affects C++ and C based OPC UA Clients and OPC UA Servers that use affected versions of the OpenSSL. Users of OpenSSL 1.0.2 should upgrade to 1.0.2zd (premium support customers only), OpenSSL 1.1.1 users should upgrade to 1.1.1n, OpenSSL 3.0 users should upgrade to 3.0.2 We strongly recommend to immediately update the OpenSSL.

Affected Products/Versions:

OpenSSL (third-party) is not part of the SDK delivery, except for evaluation editions and examples. Customers are responsible for choosing the latest OpenSSL version. All C++ and C based OPC UA SDK products, which use the affected OpenSSL versions, are affected (including .NET Core on Linux).

- **C++ based OPC UA Client Server SDK**
  (C++ SDK v1.7.6 contains example with affected OpenSSL < v1.1.1n)
- **ANSI C based OPC UA Client Server SDK**
  (AnsiC SDK 1.9.2 contains example with affected OpenSSL < v1.1.1n)
- **High Performance OPC UA SDK**
  (never contained any OpenSSL, but you most likely have used affected version)
- **UaGateway V1.5.8 and below**
  (fixed in V1.5.9 containing OpenSSL v1.1.1n)
- **UaExpert V1.6.1 and below**
  (fixed in V1.6.2 containing OpenSSL v1.1.1n)

> Important: If you are using the OPC UA components that use OpenSSL, you should immediately upgrade to OpenSSL 1.1.1n. For our Unified Automation runtime products UaExpert and UaGateway we provide new version containing latest OpenSSL v1.1.1n.

Recommendation:

- If your application uses C++ based OPC UA SDK, or AnsiC based OPC UA SDK, or High Performance SDK in combination with one of the affected OpenSSL versions you should immediately upgrade to the latest OpenSSL v1.1.1n.
- If you use the UaExpert and/or UaGateway you should immediately upgrade to the latest version containing latest OpenSSL.

FAQ:

- **Is the .NET based OPC UA Client Server SDK affected?** No, the .NET SDK does not use OpenSSL crypto library directly. However, the Linux based .NET Core edition will be affected, because it uses the system wide OpenSSL, hence you must update the OpenSSL on your Linux host system to the latest v1.1.1n immediately.