Security Risk Report

The OpenSSL Software Foundation has published security advisory regarding eight potential vulnerabilities on February 07, 2023. See https://www.openssl.org/news/secadv/20230207.txt for details. Unified Automation has conducted an analysis of the described errors with its Security Response Team. 2 issues regarding use of BIO functions are rated not remote exploitable, 3 regarding PKCS7 are rated not affected (code not used). In a nutshell: **3 out of 8** reported vulnerabilities are rated security relevant and remote exploitable, hence outlined here.

1. (CVE-2023-0286) X.400 address type confusion in X.509 GeneralName

This vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. The vulnerability can only be exploited if attacker can control certificate AND CRL. This would require admin privileges on file system or Security-Admin role permissions via UA GDS Push. We have rated the issue with CVSS v3.1 Base Score of 6.5 and a Temporal Score of 5.4 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:R)

2. (CVE-2022-4304) Timing Oracle in RSA Decryption

Bleichenbacher style timing attack on RSA decrypt to recover the pre-master secret used for the original connection Remotely exploitable, but attacker can recover only one nonce. Attacker would need to attack both sides to recover shared secret in UA Secure Conversation. When decrypting UserTokens on a None-Channel (which should not be used) it is possible to recover the RSA encrypted password. It also requires a large amount of telegrams to recover the encrypted RSA block. We have rated the issue with CVSS v3.1 Base Score of 5.9 and a Temporal Score of 4.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:R)

3. (CVE-2022-4203) X.509 Name Constraints Read Buffer Overflow (OpenSSL v3.0 to v3.0.7 only)

The buffer overrun might result in a crash which could lead to a denial of service attack. In theory it could also result in the disclosure of private memory contents. However, it is exploitable only if CA has signed the malicious cert or applications continues certificate verification after signature error. This can happen in High Performance SDK when `check_complete_chain=true` in settings.conf, which is `false` by default. We have rated the issue with CVSS v3.1 Base Score of 5.9 and a Temporal Score of 4.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:R)

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 1.0.2zg (premium support customers only), OpenSSL 1.1.1 users should upgrade to 1.1.1t, OpenSSL 3.0 users should upgrade to 3.0.8 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 v1.7.7 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 is capable of using OpenSSL v3.0)

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

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.