Security Risk Report

On July 24, 2024 during regular OPC Foundation security workgroup meeting, a possible security vulnerability was reported by Tom Tervoort of Secura B.V. (www.secura.com), which allows bypass of authentication via PKCS#1 padding oracle.

This vulnerability allows an unauthenticated attacker with network access to an OPC UA Binary TCP endpoint of a vulnerable server to bypass application authentication and gain access to the data managed by the server. Additionally the same technique could also be used to decrypt passwords or general OPC UA traffic that was previously recorded. This attack, however, exploits a known weakness of the RSA padding scheme PKCS#1, which is only used as part of the deprecated security policy “Basic128Rsa15” (deprecated by OPC Foundation, switched “off” [default] in all Unified Automation products and configurations).

Rating:

The vulnerability is rated with a Base Score of 6.8 and a Temporal Score of 6.3 according to the CVSS v3.1 metric with the following vector:

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

Details regarding prevention:

The vulnerability affects the “Basic128RSA15” security policy only. Make sure to not use the Baisc128Rsa15 not for application authentication (SecureChannel) and not for user authentication (Create/ Activate Session). In all Unified Automation OPC UA server products there is additional protection to not enable accidently. For backward compatibility however, old policy might be enabled intentionally by configuration, in that case High Performance SDK and .NET based SDK OPC UA server products will be affected.

Affected Products/Versions:

Current version of High Performance OPC UA Server SDK and .NET based OPC UA Server SDK are affected (in case Basic128Rsa15 was switched “on” intentionally).

- **.NET based OPC UA Server SDK V4.0.1 and below**
  (fixed in 4.0.2) (fixed in 3.4.3)
- **High Performance OPC UA Server SDK V1.8.1 and below**
  (fixed in 1.8.2)

Important: The vulnerable PKCS#1 padding is ONLY used in policy “Basic128Rsa15” which is deprecated and switched off by default. If NOT enabled, the CVSS score is “0” (zero).

Recommendation:

- If your UA Server application is configured to use Endpoint with “Basic128Rsa15” security policy, change your configuration and switch “off” this policy. Make sure the configuration setting “AllowDeprecatedPolicies” is disabled [default].
- If your UA Server application is configured to use UserToken with “Basic128Rsa15” security policy, change your configuration and switch “off” this policy. Make sure the configuration setting “AllowDeprecatedPolicies” is disabled [default].

FAQ:

- **Is the C++ based OPC UA Server SDK affected?** No, since v1.6.0 the C++ SDK returns constant timing on the decryption and is not affected.
- **Is the ANSI C based OPC UA Server SDK affected?** No, since v1.8.2 the AnsiC SDK returns constant timing on the decryption and is not affected.
- **Is the Runtime Product UaGateway affected?** No, since v 1.5.1 the UaGateway internally uses C++ based SDK v1.6.0 or higher which is not affected.