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 application authentication via HTTPS endpoint using signature reflection or relay.

This vulnerability allows an unauthenticated attacker with network access to an HTTPS 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 attack certificate-based user authentication. This attack requires HTTPS transport (skipping the OpenSecureChannel handshake) in combination with using a non-None SecurityPolicy for Create/Activate Session (not configured in Unified Automation SDK products). However, if configured to use secured policy over the already secured HTTPS transport, the server can be tricked to signing “nonce” data received from an unverified source.

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 HTTPS transport in combination with (any) not-None SecurityPolicy. The HTTPS transport is not released and is marked “experimental” in our source code OPC UA SDK products. Make sure to not accidentally switch “on” in CMake, hence not compile-in the experimental HTTPS transport. In all Unified Automation binary edition OPC UA server products the HTTPS transport is compiled in, but switched off [default] in configuration, make sure to not enable HTTPS endpoints accidentally. However, if compiled in, as being the case for binary edition of, C++ based SDK OPC UA, and accidentally enabled, such server products might be affected.

Affected Products/Versions:

Current version of C++ based OPC UA Server SDK is affected.

- **C++ based OPC UA Server SDK v1.8.2 and below**
  (in 1.8.3 the experimental https transport allows “None” SecurityPolicy only)
- **ANSI C based OPC UA Server SDK v1.10.0 and below**
  (not compiled-in, experimental since 1.4.0)

Important: The vulnerable requires HTTPS transport (experimental, not compiled-in), plus the combination with SecurityPolicy other than “None” (but default configuration is “None”). If NOT enabled, the CVSS score is “0” (zero).

Recommendation:

- If your UA Server application is compiled to use “experimental” feature HTTPS transport, change your CMake configuration and do not compile in this transport. It was never released for productive use.
- If your UA Server application has HTTPS transport compiled in, make sure the configuration setting only allows None-SecurityPolicy over the HTTPS transport.

FAQ:

- **Is the .NET based OPC UA Server SDK affected?** No, since v3.0.0 the .NET SDK does not contain the HTTPS transport option anymore.
- **Is the High Performance OPC UASDK affected?** No, the HP SDK never contained any https transport.
- **Is the Runtime Product UaGateway affected?** No, since v 1.6.0 the UaGateway internally uses C++ based SDK v1.8.3 or higher which is not affected.