Security Risk Report

The OPC Foundation has published CVE-2019-19135 through a Security Bulletin on March 10, 2020. See https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19135 for more information.

This vulnerability describes misbehaving servers that do not create sufficiently random numbers, which allows man in the middle attackers to reuse encrypted user credentials sent over the network. Servers having this issue will most likely create Server-Nonce being to short, not unique or not sufficiently random when asking for encrypted password credentials or signed X509 certificate credentials. The Server-Nonce is defined as unique random number of at least 32 Bytes length. Unified Automation does not use the OPC Foundation code base. UA servers created with Unified Automation OPC UA SDK's mainline version do always create sufficient random numbers of correct length.

Rating:

The vulnerability is rated with a Score of 5.4 according to the CVSS v3.1 metric with the following vector:

AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Details regarding prevention:

To prevent this vulnerability it is highly recommended to prevent interception and reuse of encrypted user credentials. As a workaround clients should only be allowed to connect to endpoints using the "Sign&Encrypt" Security Mode. To eliminate the risk, do not use "None" or "SignOnly" in combination with encrypted user credentials.

Affected Products/Versions:

- **C++ based OPC UA Server SDK before V1.5.1** (March 2016)
(since V1.5.1 the C++ Server SDK creates a unique, random ServerNonce of correct length even when the SecureChannel does not use any security)
- **ANSI C based OPC UA Server SDK before V1.4.0** (March 2014)
(since V1.4.0 the ANSI C Server SDK creates a unique, random ServerNonce of correct length whenever PKI is compiled in, since V1.6.0 ANSI C Server creates such Nonce even when no PKI was compiled in)
- **UaGateway before V 1.4.0** (March 2016)
(since V1.4.0 UaGateway internally uses the C++ Server SDK v1.5.1 and creates a unique, random ServerNonce of correct length even when the SecureChannel does not use any security)

Important: The vulnerability only exists if network communication is not encrypted. The vulnerability only affects Clients communicating with Servers which do not comply with the OPC UA specification.

Recommendation:

- If your OPC UA Server is based on or uses one of the above affected versions, you should update to the current mainline.
- Generally you should not use OPC UA Clients or OPC UA Servers that are based on components that have reached End of Life, because they are deprecated, not supported and will not be bug fixed anymore.

FAQ:

- **Is the High Performance OPC UA SDK affected?** No, the HP OPC UA Server SDK has always (since first version v1.0.0) created a sufficiently random number, if crypto support was compiled in.
- **Is the .NET based OPC UA Server SDK affected?** No, the .NET based OPC UA Server SDK has always (since first version v2.1.0) created a sufficiently random number.

Client-side Information:

UA clients that do not validate the provided random numbers may unwittingly encrypt the password in a way that allows reuse and send over the wire. UA clients should do more sophisticated validation of the provided ServerNonce before incorporating this number into encryption algorithms for password credentials or signed X509 certificate credentials. Clients should check this number for correct length (and existence) and could check for not re-using during same connection establishment. With that clients can detect the most common server-side implementation errors (detect not compliant servers). However, validating the provided ServerNonce for uniqueness and especially validating for randomness will not be reliable and hence is not implemented in Unified Automation Client SDKs.

Client-side Behavior:

- **C++ based OPC UA Client SDK before V1.5.3** (October 2016)
  (since V1.5.3 the C++ Client SDK does check for correct length and re-usage of the ServerNonce, application has the ability to override these checks)
- **High Performance OPC UA Client SDK before V1.4.0**
  (since V1.4.0 the HP Client SDK does check for correct length of the ServerNonce)
- **ANSI C based OPC UA Client SDK before V1.5.0** (June 2015)
  (since V1.5.0 the AnsiC Client SDK does check for correct length of the ServerNonce, since V1.6.0 application has the ability to override these checks)
- **.NET based Client OPC UA SDK before V2.4.1** (January 2016)
  (since V2.4.1 the .NET Client SDK does check for correct length of the ServerNonce)
- **UaGateway UA Channel before V1.4.2** (November 2016)
  (since V1.4.2 UaGateway internally uses the C++ Client SDK v1.5.3 and does check for correct length and re-usage of the ServerNonce, application has the ability to override these checks)

Recommendation:

- Clients should connect to endpoints having Security Mode “Sign&Encrypt” only, to prevent interception of credentials and replay attacks. Make sure to connect to compliant servers only.
- Generally you should not use OPC UA Clients or OPC UA Servers that are based on components that have reached End of Life, because they are deprecated, not supported and will not be bug fixed anymore.