Security Risk Report

The OPC Foundation has published CVE-2018-7559 through a Security Bulletin on April 8, 2018. See https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7559 for more information.

This vulnerability affects the handling of UserIdentityTokens when used with the Basic128Rsa15 security policy. It potentially affects all OPC UA Servers on all operating systems having the Basic128Rsa15 security policy activated in their configuration. The vulnerability allows an attacker to decrypt a previously captured password or to sign arbitrary data.

Details regarding prevention:

The vulnerability only affects OPC UA Servers that offer UserIdentityTokens encrypted with the Basic128Rsa15 security policy. This policy is deprecated by the UA Specification since July 2015, therefore it is recommended not to use this policy any longer.

The next hotfix releases of Unified Automation products will contain further fixes to eliminate the vulnerability even if the security policy Basic128Rsa15 is being used. Our OPC UA SDKs and OPC UA products will also contain additional mechanisms to prevent operators from accidentally switching on deprecated security policies. Even with these fixes a stronger security policy like Basic256Sha256 should be used instead.

Affected Products/Versions:

- **C++ based OPC UA SDK before V1.5**
  (before V1.5 the affected security policy was enabled in the default configuration)
- **ANSI C based OPC UA SDK before V1.5**
  (before V1.5 the affected security policy was enabled in the default configuration)
- **.NET based OPC UA SDK before V2.4**
  (the getting started examples still use this policy today)
- **UaGateway before V1.4**
  (and also newer UaGateways that are using old configuration settings from before V1.4)

Important: If any of these products or their default configuration are using the Basic128Rsa15 security policy, that security policy should be disabled.

Recommendation:

- If your OPC UA Server has **disabled Basic128Rsa15**, there is nothing to do.
- If your OPC UA Server has **enabled Basic128Rsa15**
  - disable it if it is not needed; even without this vulnerability the Basic128Rsa15 security policy is deprecated and should be disabled in the server configuration.
  - **C++ based UA Server:** in the server's configuration file, disable (delete) the endpoint configurations that use the affected security policy.
  - **ANSI C based UA Server:** in the server's configuration file, disable (delete) the endpoint and user token configurations that use the affected security policy.
  - **.NET based UA Server:** in the server's configuration file, disable (delete) the endpoint and user token configurations that use the affected security policy.
  - **UaGateway:** in UaGateway's "Administration Dialog" open the tab "UA Endpoints" and disable (uncheck) the affected security policy for each configured endpoint in the "Security" group box.

FAQ:

- **Are OPC UA Clients affected?** No, Clients are not affected.
- **Is the High Performance OPC UA SDK affected?** No, the HP SDK never had Basic128Rsa15 in its default configuration. Only if the Basic128Rsa15 security policy is enabled for user tokens, the HP SDK is also affected.
- **Are Java based OPC UA SDKs affected?** Yes, if using the Basic128Rsa15 security policy in combination with User Tokens, Java based OPC UA Servers are affected.
- **Is UaExpert affected?** No, the UaExpert is a Client and hence is not affected.