Security Risk Report

The OPC Foundation has published CVE-2018-12086 through a Security Bulletin on July 1, 2018. See https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12086 for more information.

This vulnerability affects clients and servers using OPC Foundation communication stack, where the decoder does not check the nesting depth of certain structures. The issue was fixed in Unified Automation OPC UA SDKs and OPC UA products a long time ago. Only customers using very old versions need to update.

Details regarding prevention:

The vulnerability affects built-in OPC UA Types that allow infinite nesting. The decoder in the OPC Foundation's OPC UA communication stack did not check the nesting depth of such structures, hence an endless recursion may occur when decoding such structure. By sending a maliciously crafted message an attacker could trigger an overflow of the call stack and crash the application of the receiver.

To prevent this vulnerability it is highly recommended to update any affected version. As a workaround clients should only be allowed to connect to known good servers. Servers would need to be protected by a firewall to allow only white-listed clients to connect.

Affected Products/Versions:

- **C++ based OPC UA SDK before V1.4.1** (June 2014)
  (this version has reached End of Life)
- **ANSI C based OPC UA SDK before V1.4.1** (May 2014)
  (this version has reached End of Life)
- **.NET based OPC UA SDK before V2.4.1** (January 2016)
  (this version has reached End of Life)
- **UaGateway before V1.4.0** (August 2015)
  (this version has reached End of Life)
- **UaExpert before V1.3.0** (June 2014)
  (this version has reached End of Life)

Important: All of the affected products were fixed long time ago. All those affected versions have reached End of Life (EOL). None of the products in their respective current mainline are affected by this vulnerable.

Recommendation:

- If your OPC UA Server or OPC UA Client is based on or uses one of the above affected version, 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 SDK comes with it's own new encoder/decoder which was not based on OPC Foundation UA-Stack. This new encoder/decoder never had any endless recursion code in it.