Security Risk Report

The XML toolkit from the GNOME project (xmlsoft.org) has published CVE-2021-3541 through a security Bulleting on Mai 13, 2021. See https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3541 for details.

The libxml2 library is a development toolbox providing the implementation of various XML standards. A flaw was found in libxml2. An exponential entity expansion attack is possible bypassing all existing protection mechanisms and leading to denial of service (DoS). The vulnerability only affects OPC UA Clients that parse XML document content by reading the content of an XML type dictionary. A specially crafted UA Server can provide this XML bomb within the XML type dictionary, which can cause the OPC UA Client to crash while parsing the XML content. UA Clients may read the XML type dictionary using C++ SDK API comfort function (on connect, on first use, never) depending on their implementation and configuration.

Rating:

The vulnerability is rated with a Base Score of 6.5 and a Temporal Score of 6.0 according to the CVSS v3.1 metric with the following vector:

AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C

Details regarding prevention:

The vulnerability is located in the third party library LibXML2. This library typically is dynamically linked to the UA Client application and can be updated by replacing the vulnerable DLL. Linux applications that use the libxml2 system library, get fixed automatically through their regular system updates.

Affected Products/Versions:

Only if you use LibXML2 before V2.9.11 and your application is configured to read/parse XML document content (e.g. OPC UA type dictionary), you are affected.

- **C++ based OPC UA SDK V1.7.4 and earlier**
  (only when using LibXML2 before V2.9.11)
- **UaExpert V1.5.2 and earlier**
  (comes with vulnerable LibXML2 V2.9.8 or earlier, can be switched off)

Important: the vulnerable component is third party library libxml2 that is dynamically linked to the software, hence can be updated/replaced independently from the application. As a workaround in UaExpert the automatic parsing/reading of XML type dictionaries can be switched off (General.TypeDictionaryMode=off, default is reconnect)

Recommendation:

- If your application uses the C++ based OPC UA Client SDK software, you may have used libxml2 version 2.9.8 or earlier, you should update the LibXML2 to V2.9.11 or higher.
- If you use UaExpert V1.5.2 (Feb 2020) or earlier, you can switch of automatic reading of type dictionary information (Settings → Configure UaExpert → General.TypeDictionaryMode = “off”). In any case you should update your UaExpert to the latest version v1.6.0 or above.

FAQ:

- **Is the .NET based OPC UA SDK affected?** No, the .NET based OPC UA SDK does not use the LibXML2 third party library for parsing XML document content.
- **Is the ANSI C based OPC UA SDK affected?** No, the ANSI C based OPC UA SDK does not contain any XML parsing functions and does not use the LibXML2 third party library.
- **Is the High Performance OPC UA SDK affected?** No, the HP SDK comes with its own XML parser, which is not capable of processing XML entities (as it is not needed by OPC UA).
- **Is the UaGateway affected?** No, even though the UaGateway may come with the vulnerable LibXML2 edition, the UaGateway is transparently passing through service calls without looking into the content, hence will no parse nor process any XML document contents of underlying UA servers.