PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

2022-12-13
2022/00011

Security Advisory for PROFINET SDK

Publication Date:	2022-12-13
Last Update:	2022-12-13
Current Version:	V1.0

Advisory Title

Vulnerabilities in XML parser library Expat (libexpat)

Advisory ID

CVE-2022-40674
CVE-2022-43680

VDE-2022-058

Vulnerability Description

Two vulnerabilities have been discovered in the Expat XML parser library (aka libexpat). This open-source component is widely used in a lot of products worldwide. An attacker could cause a program to crash, use unexpected values or execute code by exploiting these use-after-free vulnerabilities.
Profinet SDK is using XML parser library Expat as reference solution for loading the XML based Profinet network configuration files (IPPNIO or TIC).

CVE-2022-40674:
libexpat before 2.4.9 has a use-after-free in the doContent function in xmlparse.c.

CVE-2022-43680:
In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations.

Personally liable partner:
Phoenix Contact Verwaltungs GmbH
Amtsgericht Lemgo HRB 5273
Kom. Ges. Amtsgericht Lemgo HRA 3746

Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Possel-Dölken, Axel Wachholz

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDEDEXXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADEFFXXX
IBAN:
DE31 4764 0051 0226 0396 00

...

Affected products

Article no	Article	Affected versions
1175941	PROFINET SDK	<=6.6 versions, please contact your contact partner for additional information

Impact

Availability, integrity, or confidentiality of a device using the PROFINET Controller Stack might be compromised by attacks exploit these vulnerabilities.
Depending on the instantiation and timing of the defect, using previously freed memory might result in a variety of negative effects, from the corruption of valid data to the execution of arbitrary code. In the default installation a vulnerable libexpat is present, but it may have been replaced in the toolchain itself.

Classification of Vulnerability

CVE-2022-40674
Base Score: 9.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE-416: Use After Free

CVE-2022-43680
Base Score: 7.5
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE-416: Use After Free

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

Temporary Fix / Mitigation

We strongly recommend customers to ensure that only data from reliable sources is used. Affected customers should also check if vulnerable libexpat library versions are used in the specific configuration tool chain.

For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note:

Measures to protect network-capable devices with Ethernet connection

Remediation

1. Update configuration tool chains to libexpat library version 2.4.9. or higher.

...

2. Upgrade to PROFINET SDK 6.7 or higher if necessary.

Acknowledgement

We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

History

V1.0 (2022-12-13): Initial publication