PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

30 March 2022
300543539

Security Advisory for PROFINET SDK

Advisory Title

Several vulnerabilities in XML parser library Expat (aka libexpat)

Advisory ID

CVE-2021-46143, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824
CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-23852
CVE-2022-23990, CVE-2021-45960, CVE-2022-25315, CVE-2022-25314
CVE-2022-25313, CVE-2022-25235, CVE-2022-25236

VDE-2022-005

Vulnerability Description

Several 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.
A remote, anonymous attacker could use an integer overflow, uncontrolled resource consumption, improper encoding, escaping of output or exposure of resource to wrong sphere to execute arbitrary program code when loading specially crafted XML files.

Profinet SDK is using XML parser library Expat as reference solution for loading the XML based Profinet network configuration files (IPPNIO or TIC).

Integer overflow (CWE-190):

CVE-2021-46143:
In doProlog in xmlparse.c in Expat before 2.4.3, an integer overflow exists for m_groupSize

CVE-2022-22822:
AddBinding in xmlparse.c in Expat before 2.4.3 has an integer overflow.

CVE-2022-22823:
Build_model in xmlparse.c in Expat before 2.4.3 has an integer overflow.

CVE-2022-22824:
DefineAttribute in xmlparse.c in Expat before 2.4.3 has an integer overflow.

CVE-2022-22825:
Lookup in xmlparse.c in Expat before 2.4.3 has an integer overflow.

CVE-2022-22826:
NextScaffoldPart in xmlparse.c in Expat before 2.4.3 has an integer overflow.

CVE-2022-22827:
StoreAtts in xmlparse.c in Expat before 2.4.3 has an integer overflow.

CVE-2022-23852:
Expat before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES

CVE-2022-23990:
Expat before 2.4.4 has an integer overflow in the doProlog function.

CVE-2022-25315
In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.

CVE-2022-25314
In Expat (aka libexpat) before 2.4.5, there is an integer overflow in copyString

Uncontrolled Resource Consumption ('Resource Exhaustion') (CWE-400):

CVE-2021-45960:
In Expat before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).

CVE-2022-25313
In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth in the DTD element

Improper Encoding or Escaping of Output (CWE 116):

CVE-2022-25235
Xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context.

Exposure of Resource to Wrong Sphere (CWE 668):

CVE-2022-25236
Xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs

Affected products

Article no	Article	Affected versions
1175941	PROFINET SDK	>= 6.0 & < 6.6

Impact

Availability, integrity, or confidentiality of a device using the PROFINET Controller Stack might be compromised by attacks exploit these vulnerabilities. If specially crafted Profinet network configuration files (IPPNIO or TIC) are loaded during the Profinet startup an integer overflow leads to a buffer overflow which enables the attacker to elevate privileges and obtain access to the device. The attacker may take over the system, steal data or prevent a system or application to run correctly.
The PROFINET Device Stack provides an optional configuration possibility via the above-mentioned files and might be vulnerable when this dedicated use case is supported.

Classification of Vulnerability

Integer overflow (CWE 190)
(up to): Base Score: 9.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Uncontrolled Resource Consumption ('Resource Exhaustion') (CWE-400):
Base Score: 8.8
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Improper Encoding or Escaping of Output (CWE 116):
Base Score: 9.8
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

...

Exposure of Resource to Wrong Sphere (CWE 668):
Base Score: 9.8
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Temporary Fix / Mitigation

The PROFINET SDK includes an Engineering tool as reference solution to generate Profinet configuration IPPNIO or TIC XML files. This configuration is transferred to a device running the Profinet stack and loaded during startup of the Profinet stack.

When the IPPNIO or TIC files are transferred via an untrusted environment (e.g.: Network or e-Mail, …) an attacker knowing these vulnerabilities mentioned above might manipulate the files in a specific way to gain access to the device.

To mitigate these vulnerabilities the integrity and authenticity of the configuration data it must be ensured by transferring the data only via trusted connections.

Advice's how to ensure trusted connections can be found in the following document:
Measures to protect network-capable devices with Ethernet connection

Companies which are using their own configuration system instead of the reference solution are not affected as long they don't utilize the related libexpat library.

We kindly advise you to check if in your specific configuration tool chain, the libexpat library is used or version number is 2.4.6. or higher.

Remediation

1. Use only trusted connections between the Engineering tools and the devices executing the Profinet stack.

2. Update configuration tool chains to libexpat library version 2.4.6. or higher.

3. Upgrade to PROFINET SDK 6.6 or higher if necessary.

Acknowledgement

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