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

22 March 2022
300543707 / 300545395

Security Advisory for PLCnext Technology Toolchain and FL Network Manager

Advisory Title

Path Traversal in SharpZipLib
CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Advisory ID

CVE-2021-32840
CVE-2021-32842
VDE-2022-007

Vulnerability Description

SharpZipLib (or #ziplib) is a Zip, GZip, Tar and BZip2 library. Prior to version 1.3.3, a TAR file entry ../evil.txt may be extracted in the parent directory of destFolder. This leads to arbitrary file write that may lead to code execution. The vulnerability was fixed in SharpZipLib version 1.3.3.

Affected products

Article no	Article	Affected versions	Fixed Version
-	PLCnext Technology tool chain for Windows including Eclipse Add-in, Microsoft Visual Studio Extension for C++ and C#.	>=2019.0 LTS & < 2022.0 LTS	Download
2702889	FL Network Manager	>= 4.0 & <= 6.0	Download

...

Impact

SharpZipLib is used in PLCnext CLI for the SDK installation on Windows.
Via a specially crafted “zip file” an attacker could take over a vulnerable PC, gain unauthorised access to sensitive data, or affect the availability of the system.

In FL Network Manager SharpZipLib is used for opening device snapshots.
A snapshot file contains, for example, information about the device status, the device configuration, an event log, etc. The snapshot file is a zip archive with the prefix "snapshot" and the extension "tar.gz". This zip file helps Phoenix Contact to solve problems with the device.
The client may choose arbitrary files used as a snapshot. If the snapshot is compromised it may lead to code execution described in the vulnerability section.

Classification of Vulnerability

Base Score:9.8 critical
Vector: CVSS:3.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Remediation

PHOENIX CONTACT strongly recommends updating the PLCnext Technology tool chain for Windows to Version 2022.0 LTS or higher, which fixes this vulnerability and can be downloaded from the download area (Software) of your PLCnext Controller.

Please use the Device Snapshots only from safe sources and ensure data integrity or update the FL Network Manager to Version 6.0.1 or higher.

Acknowledgement

This vulnerability was discovered and reported by GHSL team member @JarLob (Jaroslav Lobačevski). 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.