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

08 August 2023
2023/00012

Security Advisory for PLCnext Engineer

Publication Date:	2023-08-08
Last Update:	2023-08-08
Current Version:	V1.0

Advisory Title

Vulnerabilities in LibGit2Sharp/LibGit2.

Advisory ID

CVE-2018-11235, CVE-2019-1348, CVE-2019-1349, CVE-2019-1350, CVE-2019-1351, CVE-2019-1352, CVE-2019-1353, CVE-2019-1354, CVE-2019-1387, CVE-2022-24765, CVE-2022-29187

VDE-2023-016

Vulnerability Description

Several vulnerabilities have been discovered in the LibGit2Sharp or underlying LibGit2 library. This open-source component is widely used in a lot of products worldwide.
The product is vulnerable to remote code execution, privilege escalation and tampering.
PLCnext Engineer is using the LibGit2Sharp library to provide version control capabilities.

Personally liable partner:
Phoenix Contact Verwaltungs-GmbH
Management office Blomberg
Distr. court Lemgo HRB 10904
Statutory seat Vaduz/Liechtenstein
Comm. reg. FL-0002.700.066-3
GmbH & Co. KG:
Distr. court 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

...

Improper Input Validation (CWE-20):

CVE-2019-1349
By using NTFS 8.3 short names, backslashes or alternate file streams, it is possible to cause submodules to be written into pre-existing directories during a recursive clone using git.

CVE-2019-1350
Recursive clones may lead to arbitrary remote code executing due to improper quoting of command line arguments.

CVE-2019-1352
By using NTFS-style alternative file streams for the ".git" directory, it is possible to overwrite parts of the repository. While this has been fixed in the past for Windows, the same vulnerability may also exist on other systems that write to NTFS filesystems.

CVE-2019-1354
On Windows, backslashes are not a valid part of a filename but are instead interpreted as directory separators. As other platforms allowed to use such paths, it was possible to write such invalid entries into a Git repository and was thus an attack vector to write into the ".git" directory.

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

CVE-2018-11235
Remote code execution can occur. With a crafted ".gitmodules" file, a malicious project can execute an arbitrary script on a machine that runs "git clone --recurse-submodules" because submodule "names" are obtained from this file, and then appended to $GIT_DIR/modules, leading to directory traversal with "../" in a name. Finally, post-checkout hooks from a submodule are executed, bypassing the intended design in which hooks are not obtained from a remote server.

Improper Ownership Management (CWE-282):

CVE-2022-29187
Vulnerability to privilege escalation in all platforms.

Uncontrolled Search Path Element (CWE-427):

CVE-2022-24765
This vulnerability affects users working on multi-user machines, where untrusted parties have write access to the same hard disk.

CVE-2022-29187
Vulnerability to privilege escalation in all platforms.

Use of Incorrectly Resolved Name or Reference (CWE-706):

...

CVE-2019-1351
Windows provides the ability to substitute drive letters with arbitrary letters, including multi-byte Unicode letters. While the only permitted drive letters for physical drives on Windows are letters of the US-English alphabet, this restriction does not apply to virtual drives assigned via subst <letter>:<path>. Git mistook such paths for relative paths, allowing writing outside of the work tree while cloning.

CWE under investigation:

CVE-2019-1348
The --export-marks option of git fast-import is exposed also via the in-stream command feature export-marks=... and it allows overwriting arbitrary paths.

CVE-2019-1387
It is possible to let a submodule's git directory point into a sibling's submodule directory, which may result in overwriting parts of the Git repository and thus lead to arbitrary command execution.

CVE-2019-1353
By using NTFS-style 8.3 short names, it was possible to write to the ".git" directory and thus overwrite parts of the repository, leading to possible remote code execution. While this problem was already fixed in the past for Windows, other systems accessing NTFS filesystems are vulnerable to this issue too.

Affected products

Article no	Article	Affected versions
1046008	PLCnext Engineer	<= 2023.3

Impact

Availability, integrity, or confidentiality of PLCnext Engineer might be compromised by attacks exploiting these vulnerabilities. Specially crafted git configuration files lead to a remote code execution which enables the attacker to elevate privileges and obtain access to the application. The attacker may take over the system, steal data or prevent a system or application from running correctly.

...

Classification of Vulnerabilities

Improper Input Validation (CWE-20)
CVE-2019-1349
(Up to): Base Score: 8.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE-2019-1350
(Up to): Base Score: 8.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE-2019-1352
(Up to): Base Score: 8.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE-2019-1354
(Up to): Base Score: 8.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22)
CVE-2018-11235
(Up to): Base Score: 7.8
Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Improper Ownership Management (CWE-282)
CVE-2022-29187
(Up to): Base Score: 7.8
Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Uncontrolled Search Path Element (CWE-427)
CVE-2022-24765
(Up to): Base Score: 7.8
Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2022-29187
(Up to): Base Score: 7.8
Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Use of Incorrectly-Resolved Name or Reference (CWE-706)
CVE-2019-1351
(Up to): Base Score: 7.5
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CWE under investigation:
CVE-2019-1348

...

(Up to): Base Score: 3.3
Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVE-2019-1387
(Up to): Base Score: 8.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE-2019-1353
(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

Temporary Fix / Mitigation

To mitigate the aforementioned vulnerabilities, the integrity and authenticity of the git configuration data must be ensured. Otherwise, we kindly advise you to refrain from using the version control feature in version lower than 2023.6.

Remediation

Phoenix Contact strongly recommends updating PLCnext Engineer to version 2023.6 or higher.

Acknowledgement

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

History

V1.0 (2023-08-08): Initial publication