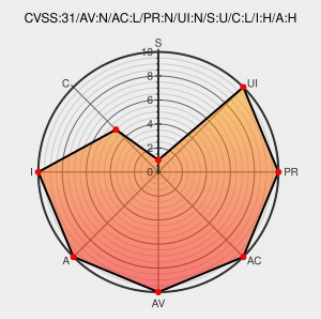
CVE-2020-8768

Published on: 02/17/2020 12:00:00 AM UTC

Last Modified on: 01/01/2022 07:38:00 PM UTC

CVE-2020-8768

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ilc 2050 Bi from Phoenixcontact contain the following vulnerability:

An issue was discovered on Phoenix Contact Emalytics Controller ILC 2050 BI before 1.2.3 and BI-L before 1.2.3 devices. There is an insecure mechanism for read and write access to the configuration of the device. The mechanism can be discovered by examining a link on the website of the device.

CVE-2020-8768 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.4 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
PHOENIX CONTACT Emalytics Controller ILC 2050 BI(L) allows unauthorised read and write access to the configuration file. — German (Germany)	Third Party Advisory cert.vde.com text/html	MISC cert.vde.com/de-de/advisories/vde-2020-001

PHOENIX CONTACT Emalytics Controller ILC | CISA

www.us-cert.gov
text/html

MISC www.us-cert.gov/ics/advisories/icsa-20-063-02

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

590570 PHOENIX CONTACT Emalytics Controller ILC Incorrect Permission Assignment for Critical Resource Vulnerability (ICSA-20-063-02)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Phoenixcontact	Ilc 2050 Bi	-	All	All	All
Hardware	Phoenixcontact	Ilc 2050 Bi	-	All	All	All
Hardware	Phoenixcontact	Ilc 2050 Bi-l	-	All	All	All
Hardware	Phoenixcontact	Ilc 2050 Bi-l	-	All	All	All
Operating System	Phoenixcontact	Ilc 2050 Bi-l Firmware	All	All	All	All
Operating System	Phoenixcontact	Ilc 2050 Bi-l Firmware	All	All	All	All
Operating System	Phoenixcontact	Ilc 2050 Bi Firmware	All	All	All	All
Operating System	Phoenixcontact	Ilc 2050 Bi Firmware	All	All	All	All

cpe:2.3:h:phoenixcontact:ilc_2050_bi:-:*:*:*:*:*:*:*:

cpe:2.3:h:phoenixcontact:ilc_2050_bi:-:*:*:*:*:*:*:*:

cpe:2.3:h:phoenixcontact:ilc_2050_bi-l:-:*:*:*:*:*:*:*:

cpe:2.3:h:phoenixcontact:ilc_2050_bi-l:-:*:*:*:*:*:*:*:

cpe:2.3:o:phoenixcontact:ilc_2050_bi-l_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:phoenixcontact:ilc_2050_bi-l_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:phoenixcontact:ilc_2050_bi_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:phoenixcontact:ilc_2050_bi_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report