



CVE-2021-33541

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-33541
State	PUBLIC
Assigner	info@cert.vde.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-25 19:15:00 UTC
Updated	2021-07-02 00:11:00 UTC
Description	Phoenix Contact Classic Line Controllers ILC1x0 and ILC1x1 in all versions/variants are affected by a Denial-of-Service vul

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Phoenixcontact	Ilc1x0	-	All	All	All
Operating System	Phoenixcontact	Ilc1x0 Firmware	All	All	All	All
Hardware	Phoenixcontact	Ilc1x1	-	All	All	All
Operating System	Phoenixcontact	Ilc1x1 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
PHOENIX CONTACT : Security Advisory for ILC1x1 Industrial controllers — English (USA)	CONFIRM	cert.vde.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: This vulnerability was discovered by the Industrial Control Security Laboratory of Qi An Xin Technology Group Inc. from China and reported to CERT@VDE. PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)