

07 June 2021
300502414

Security Advisory for FL COMSERVER UNI

Advisory Title

A Denial of Service vulnerability was discovered in firmware V2.40 of FL COMSERVER UNI products.

Advisory ID

CVE-2021-21002
VDE-2021-022

Vulnerability Description

When the communication partner sends an invalid Modbus exception response to the FL COMSERVER UNI as a query, the Modbus communication stops, and the device will be unresponsive for some minutes before the functionality is fully restored (CWE-772).

Affected products

Article no	Article	Affected versions	Fixed version
2313452	FL COMSERVER UNI 232/422/485	< 2.40	2.41
2904817	FL COMSERVER UNI 232/422/485-T	< 2.40	2.41

Impact

An attacker may use this vulnerability to execute a Denial of Service (DoS) attack.

Classification of Vulnerability

Base Score: 7.5

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Personally liable partner:
Phoenix Contact Verwaltungs GmbH
Amtsgericht Lemgo HRB 5273
Kom. Ges. Amtsgericht Lemgo HRA 3746Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Pessel-Dölken, Axel WachholzDeutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDE33XXX
IBAN:
DE93 3607 0050 0226 2665 00Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADE33XXX
IBAN:
DE31 4764 0051 0226 0396 00

Remediation

PHOENIX CONTACT recommends affected users to upgrade to the latest firmware version which is available for download.

Acknowledgement

This vulnerability was found by Petri Tuomio and reported to PHOENIX CONTACT by Wärtsilä PSIRT.

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.