PEPPERL+FUCHS Your automation, our passion.

CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: Multiple DTM and VisuNet Software – Vulnerability may allow local authorized attackers access and remote code execution on the target device

Document ID TDOCT-7494_ENG
Publication date 2021-10-25

Vulnerabilities

Identifier	Vulnerability Type	Description
CVE-2018-1285	CWE-611: Improper Restriction of XML External Entity Reference	Apache log4net versions before 2.0.10 do not disable XML external entities when parsing log4net configuration files. This allows for XXE-based attacks in applications that accept attacker-controlled log4net configuration files.

Severity

Identifier	Base Score and Vector
CVE-2018-1285	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected DTM products

Item	Item Version	DTM / Component	DTM / Component Version
FieldConnex DTM Collection	1.7.0.2146 and previous	HD2-GTR-4PA DTM	2.0.5 to 2.0.12.2146
		HD2-GTR-4PA.PN DTM	1.0.4.2146 and previous
		PROFINET IO Communication DTM	1.0.4.2146 and previous
		D0-MIO-Ex12.PA. DTM	1.0.3.2146 and previous
		D0-TI-Ex8.PA. DTM	1.1.3.2146 and previous
		ARS11-*-*-* DTM	1.0.1.2146 and previous
Honeywell Integration Package	1.1.2.0 and previous	ADM Project Builder Honeywell	1.0.2.1418 and previous
		FieldConnex Diagnostic ActiveX	2.2.2.3478 and previous
		FieldConnex Diagnostic Server	2.2.2.3086 and previous
Emerson Integration Package	N/A	ADM Project Builder Emerson	1.1.3.1463 and previous
		AMS Alert Adapter	1.1.2.69 and previous

Item	Item Version	DTM / Component	DTM / Component Version
Diagnostic Manager	2.0.0.1177 to 2.2.2.3478	All contained DTMs	2.0.0.1177 to 2.2.2.3478
FieldConnex Diagnostic Gateway FF DTM	2.2.2.3478 and previous	All contained DTMs	2.2.2.3478 and previous
FDH-1 Manager	1.0.1.1022 and previous	N/A	N/A
ABB Project Builder	1.1.1.1122 and previous	N/A	N/A
DTM Collection HART-Multiplexer	2.0.0.130 and previous	All contained DTMs	N/A
TMI-FF DTM	2.6.3.10 and previous	All contained DTMs	N/A
HART DTM Library Enhanced used with PS3500-DM	2.4.11.26 and previous	All contained DTMs	N/A
DTM used with S1SD-1TI-1U	N/A	P+F DTMLibrary Modbus	V2.3.4.68
DTM Library HART used with 6500 Series	2.4.11.59 and previous	All contained DTMs	N/A
DTM Collection Level Control Technology used with Level Radar LCR20, LTC50, LTC51, LRC57	1.0.31 and previous	All contained DTMs	N/A
DTM Collection WirelessHART	1.0.2.4 and previous	All contained DTMs	N/A

Affected VisuNet products

Item	Version
VisuNet RM Shell	5.5.0 and previous
VisuNet Factory Reset	5.x
VisuNet Factory Reset	6.1.0 and previous
VisuNet Control Center	4.7.1 and previous
VisuNet GXP PC Service Tool	1.1.0 and previous

Summary

Critical vulnerabilities have been discovered in the utilized component log4net by Apache Software Foundation.

Impact

Pepperl+Fuchs analyzed and identified affected devices.
In table “Affected products” packages are listed next to some products, this means that the products are only affected if the corresponding software is installed since the package implements the vulnerability.

To exploit the vulnerability, the access rights of an authorized user or admin are required.

The impact of the vulnerability on the affected products may result in

- denial of service
- loss of credentials
- code execution

The CVSS environmental score is specific to the customer's environment and should therefore be individually assessed by the customer to accomplish final scoring.
The original CVE refers to a network access scenario. With our products, it is a local access scenario. For this reason, the risk of exploiting this vulnerability is reduced.

Solution

The following affected DTM products can be updated to the listed version:

Item	Version
FieldConnex DTM Collection	1.7.1.2159
Diagnostic Manager	2.2.3.3527
FieldConnex Diagnostic Gateway FF DTM	2.2.3.3527
FDH-1 Manager	1.0.2.1049
ABB Project Builder	1.1.2.1134
Honeywell Integration Package	1.1.3.0
Emerson Integration Package [ADM Project Builder Emerson]	1.1.4.1474
Emerson Integration Package [AMS Alert Adapter]	1.1.3.72
DTM Collection HART-Multiplexer	2.0.1.208

External countermeasures are needed for the remaining products.
The following protective measure is required for VisuNet devices and the PCs/Servers with an installed DTM:

- Restrict local access to the device, PC/Server and use user authentication to prevent unauthorized access.

Reported by

CodeWrights GmbH
Coordinated by CERT@VDE

Support

For support please contact your local Pepperl+Fuchs sales representative.