Yokogawa Security Advisory Report

YSAR-15-0001
Published on February 16, 2015
Last updated on December 25, 2017

YSAR-15-0001: Buffer overflow vulnerability in YOKOGAWA HART Device DTM

Overview:

A buffer overflow vulnerability has been found with some YOKOGAWA HART Device Type Manager (DTM). Yokogawa identified the range of products that could be influenced by the vulnerability in this document.

Go over the report and confirm which products are affected in order to consider security measures for the overall systems. Also please consider applying the countermeasures as needed.

Affected HART Device DTMs for Products:

The vulnerability exists in the HART Device DTMs for the following devices with each Device Revision(s) listed below. These devices do not have the vulnerability described in the present report, but the HART Device DTMs do when they are launched on PC with the corresponding hardware online.

- ADMAG AE Series Magnetic Flowmeters (AE/AE14) (Rev.1,2)
- ADMAG SE Series Magnetic Flowmeters (SE/SE14) (Rev.1,2)
- AM11 Magnetic Flowmeter Remote Converter (Rev.1)
- AXFA11 Magnetic Flowmeter Remote Converter (Rev.1)
- ADMAG AXF Series Magnetic Flowmeters (AXF/AXFA14) (Rev.1)
- ADMAG AXR Two-wire Magnetic Flowmeters (Rev.1,2)
- digitalYEWFLO Vortex Flowmeter (Rev.1,2,3,4)
- Dpharp EJA /EJA-A Series Pressure Transmitters/Differential PressureTransmitters (Rev.1,2,3)
- Dpharp EJX Series Pressure Transmitters/Differential PressureTransmitters (Rev.1,2,3)
- EJX Multivariable Transmitters (EJX910A/EJX930A) (Rev.1,2)
- Rotameter (Rev.1)
- Coriolis Mass Flowmeters- ROTAMASS 3-Series(RCCT3x/RCCF31) (Rev.1,2,3)
- Coriolis Mass Flowmeters(CF11) (Rev.1)
- Differential Pressure Transmitters (Rev.1)
- YEWFLO Vortex Flowmeter (Rev.1,2)
- YT200 Temperature Transmitters (Rev.1)
- YTA110/YTA310/YTA320 Temperature Transmitters (Rev.1,2,3)
- YTA70 Temperature Transmitters (Rev.1)
- AV550G (Rev.1)
- DO202 (Rev.1)
- ISC202 (Rev1) / ISC450 (Rev.1,2) /PH150 (Rev.1,2) /PH202 (Rev.1) /PH450 (Rev.1,2) /SC150 (Rev.1,2) /SC202 (Rev.1) / SC450 (Rev.1,2)
- ZR202 (Rev.1) /ZR402 (Rev.1)

Products containing the HART Device DTMs:

DeviceFiles bundled with the following software products contains the HART Device DTMs which have above vulnerability

.

- PRM (from R3.02 to R3.20)
- FieldMate (from R1.02.00 to R3.01.10)
- EJXMVTool (from R1.02 to R1.03) / FlowNavigator (from R1.04 to R1.05)

- DeviceFiles and Yokogawa DTMCollection HART that has been delivered through the below URL also contains the HART Device DTMs which have above vulnerability.
  https://partner.yokogawa.com/global/fieldmate/
  http://downloads.yokogawa-europe.com/login.aspx?ReturnUrl=%2fdefault.aspx

Vulnerability:

By sending specially crafted response packets to the 4-20mA current loop, the DTM component and the FDT Frame application becomes unresponsive.

The risk of exploiting this vulnerability could be low because the attack requires compromised access to the 4-20mA current loop and timing the spoofed response.

CVSS Base Score: 1.8, Temporal Score: 1.5

Access Vector (AV)	Local (L)	Adjacent Network (A)		Network (N)
Access Complexity (AC)	High (H)	Medium (M)		Low (L)
Authentication (Au)	Multiple (M)	Single (S)		None (N)
Confidentiality Impact (C)	None (N)	Partial (P)		Complete (C)
Integrity Impact (I)	None (N)	Partial (P)		Complete (C)
Availability Impact (A)	None (N)	Partial (P)		Complete (C)

Exploitability (E)	Unproven (U)	Proof-of-Concept(POC)	Functional (F)	High (H)	Not Defined (ND)
Remediation Level (RL)	Official Fix (OF)	Temporary Fix (TF)	Workaround (W)	Unavailable (U)	Not Defined (ND)
Report Confidence (RC)	Unconfirmed (UC)	Uncorroborated (UR)	Confirmed (C)	Not Defined (ND)	

Countermeasures:

Please contact the supports in the following section for the countermeasures regarding the affected products.

Yokogawa strongly suggests all customers to introduce appropriate security measures not only for the vulnerabilities identified but also to the overall systems.

Supports:

For questions related to this document, please contact the below.

- Field Instruments, FieldMate, EJXMVTool, FlowNavigator
  https://contact.yokogawa.com/cs/gw?c-id=000609
- PRM
  https://contact.yokogawa.com/cs/gw?c-id=000099

Reference:

1. A Complete Guide to the Common Vulnerability Scoring System (CVSS)
   http://www.first.org/cvss/cvss-guide.pdf
   CVSS is a common language for scoring IT vulnerabilities independent from any vendors. It provides an open framework for communicating the characteristics and impacts of IT vulnerabilities, scaling it in numeric scores.
   The CVSS scores described in this report are provided "AS IS." Yokogawa has no guarantee over the scores, and the severity caused by the vulnerabilities has to be judged by the users considering the security measures equipped with the overall systems.

2. ICS-CERT Advisory : ICSA-15-012-01
   https://ics-cert.us-cert.gov/advisories/ICSA-15-012-01

Revision History:

February 16, 2015	1st Edition
November 11, 2015	2nd Edition: Update the revision of PRM containing affected HART Device DTM
December 25, 2017	3rd Edition: URLs in Products containing the HART Device DTMs and Supports are updated.

* Contents of this document are subject to change without notice.