Yokogawa Security Advisory Report

YSAR-15-0001

公開日 2015-02-16
最終更新日 2015-11-11

YSAR-15-0001: 横河製品の HART Device DTM にバッファオーバーフローの脆弱性

概要:

一部の横河製品の HART Device Type Manager (DTM) にバッファオーバーフローの脆弱性が存在することを確認しました。以下に、この脆弱性の影響を受ける製品をご案内いたします。
本レポートの内容をご確認の上、影響を受ける製品を含むシステム全体のセキュリティ対策などを総合的にご判断いただき、必要に応じて対策の適用をご検討ください。

影響を受ける製品の HART Device DTM:

下記製品(および、デバイスレビジョン)に対応した HART Device DTM に脆弱性が存在します。
下記製品自体はデバイスレビジョンに関係なく本レポートに記載しています脆弱性はありません。下記製品に対して HART Device DTM を起動し、機器と接続した場合に本レポートの脆弱性の影響を受けます。

- 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)

上記 HART Device DTM を含む製品:

下記製品に同梱されている DeviceFiles は上記脆弱性が存在する HART Device DTM を含んでいます。

- PRM (R3.02 から R3.20)
- FieldMate (R1.02.00 から R3.01.10)

- EJXMVTool (R1.02 から R1.03) / FlowNavigator （R1.04 から R1.05）

- また、下記の URL で配信していた DeviceFiles、および、Yokogawa DTMCollection HART にも含まれます。
  https://fieldmate.yokogawa.co.jp/PMK/Top.do?lang=ja
  http://downloads.yokogawa-europe.com/login.aspx?ReturnUrl=%2fdefault.aspx

脆弱性詳細:

4-20mA カレントループにおいて細工されたレスポンスパケットを送信することで、DTM コンポーネントおよび FDT フレームアプリケーションを停止させることができてしまいます。

ただし、攻撃実行には 4-20mA カレントループへの不正なアクセス、およびレスポンスのタイミングでのパケット送信が必要であることから、今回確認された脆弱性が悪用されるリスクは少ないと考えられます。

CVSS における本脆弱性の基本値は 1.8、現状値は 1.5 です。

攻撃元区分(AV)	ローカル(L)	隣接(A)		ネットワーク(N)
攻撃条件の複雑さ(AC)	高(H)	中(M)		低(L)
攻撃前の認証要否(Au)	複数(M)	単一(S)		不要(N)
機密性への影響(C)	なし(N)	部分的(P)		全面的(C)
完全性への影響(I)	なし(N)	部分的(P)		全面的(C)
可用性への影響(A)	なし(N)	部分的(P)		全面的(C)

攻撃される可能性(E)	未実証(U)	実証可能(POC)	攻撃可能(F)	容易に攻撃可能(H)	未評価(ND)
利用可能な対策レベル(RL)	正式(OF)	暫定(TF)	非公式(W)	なし(U)	未評価(ND)
脆弱性情報の信頼性(RC)	未確認(UC)	未確証(UR)	確認済(C)	未評価(ND)	

対策方法:

影響を受ける製品の対策方法については下記サポートまでお問い合わせください。

なお、今回確認された脆弱性に限らず、システム全体において適切なセキュリティ対策を講じていただくことを推奨しています。

サポート:

本レポートの内容に関するご質問等については、下記にお問い合わせください。
・フィールド機器, FieldMate, EJXMVTool, FlowNavigator
https://plus.yokogawa.co.jp/gw/gw.po?c-id=000608
・PRM
https://plus.yokogawa.co.jp/gw/gw.po?c-id=000146

参考:

1. CVSS(共通脆弱性評価システム)について
   http://www.ipa.go.jp/security/vuln/CVSS.html
   共通脆弱性評価システム CVSS (Common Vulnerability Scoring System) は、情報システムの脆弱性に対するベンダーに依存しない汎用的な評価手法です。脆弱性の深刻度を同一の基準の下で定量的に比較できるようになります。
   本レポートに記載されている CVSS の各値は現状のまま提供するものであり、いかなる保証も伴いません。本レポートに記載されている脆弱性が実際にどれだけの深刻度があるかについては、影響を受ける製品を含むシステム全体のセキュリティ対策などを総合的に判断した上で、お客様自身で評価していただく必要があります。

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

更新履歴:

2015-02-16	初版
2015-11-11	第 2 版 : 影響を受ける HART Device DTM を含む PRM のレビジョンを更新

※本ドキュメントの内容については、将来予告なしに変更することがあります。