公開日　2023 年 03 月 17 日
株式会社コンテック

CONPROSYS IoT ゲートウェイの脆弱性について

■概要

当社製の IoT ゲートウェイ「CONPROSYS M2M Gateway」「CONPROSYS M2M コントローラ」（以下 CONPROSYS IoT ゲートウェイ）において複数の脆弱性が存在することが判明しました。本脆弱性を悪意ある攻撃者に悪用された場合、データの盗用や改竄、悪意のあるプログラムを実行しシステムを破壊される等の影響を受ける恐れがあります。

この問題の影響を受ける製品と対策方法、回避策を以下に示します。対策または回避策の実施をお願いいたします。

■該当製品

製品名　　：CONPROSYS M2M Gatewayシリーズ、M2Mコントローラシリーズ
型式　　：

① M2M Gateway(5機種)
CPS-MG341-ADSC1-111、CPS-MG341-ADSC1-931、CPS-MG341G-ADSC1-111、CPS-MG341G-ADSC1-930、CPS-MG341G5-ADSC1-931

② M2Mコントローラ コンパクトタイプ(9機種)
CPS-MC341-ADSC1-111、CPS-MC341-ADSC1-931、CPS-MC341-ADSC2-111、CPS-MC341G-ADSC1-110、CPS-MC341Q-ADSC1-111、CPS-MC341-DS1-111、CPS-MC341-DS11-111、CPS-MC341-DS2-911、CPS-MC341-A1-111

③ M2Mコントローラ スタックタイプ(5機種)
CPS-MCS341-DS1-111、CPS-MCS341-DS1-131、CPS-MCS341G-DS1-130、CPS-MCS341G5-DS1-130、CPS-MCS341Q-DS1-131

バージョン：① Ver.3.7.10以下
② Ver.3.7.6 以下
③ Ver.3.8.8 以下

■判明した脆弱性と脆弱性がもたらす脅威

【JVNVU#96198617】

① CVE-2023-27917:「CONPROSYS IoT ゲートウェイにおける OS コマンドインジェクション」
ネットワーク確認画面から OS が実行できるコマンドを入力することができ、管理画面にログイン可能な悪意ある攻撃者に利用されることで情報の盗用・改竄、システムの破壊、悪意あるプログラムの実行等が行われる可能性があります。
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H　基本値：8.8

② CVE-2023-27389:「CONPROSYS IoT ゲートウェイにおける不十分な暗号強度」
本製品のソフトウェアの更新に用いるファイルの暗号強度が不十分なため、
ファイルが解析可能な状態となっており、悪意のあるファームウェアに差し替えること

でシステムの改竄、破壊、悪意のあるプログラムを実行する可能性があります。
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H　基本値：6.6

③ CVE-2023-23575:「CONPROSYS IoT ゲートウェイにおけるアクセス制限不備」
管理者権限でのみアクセス可能なネットワーク確認画面が通常権限のユーザーでもアクセスできる状態となっており、悪意ある攻撃者に利用されることでネットワーク情報の盗用等が行われる可能性があります。
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N　基本値：4.3

■対策方法

コンテックの Web サイトにある最新のファームウェアに更新することで上記脆弱性の対策を施したバージョンを利用可能です。
コンテック サイトからのダウンロードページ：

① M2M Gateway
https://www.contec.com/jp/download/donwload-list/?itemid=f832c526-dcf6-4976-85aa-f536c15a8120#firmware

② M2M コントローラ コンパクトタイプ
https://www.contec.com/jp/download/donwload-list/?itemid=a054b3eb-da97-40d0-9598-d7f5ff4239ec#firmware

③ M2M コントローラ スタックタイプ
https://www.contec.com/jp/download/donwload-list/?itemid=a1b33f0d-d32b-4549-9741-613cd37d5528#firmware

■回避策

対策バージョンに更新できないお客様に対し、これらの脆弱性が悪用されるリスクを最小限に抑えるために、当社は以下に示す回避策を講じることを推奨します。

・本製品のネットワークの上流側にファイアウォールを設置する
・本製品のネットワークアクセスを信頼できる閉域網で構成する
・本製品のユーザー・パスワード設定を出荷時から変更する
・本製品のユーザー・パスワード設定を定期的に変更する

■関連情報

・JVNVU#96198617「コンテック製 CONPROSYS IoT ゲートウェイにおける複数の脆弱性」
https://jvn.jp/vu/JVNVU96198617/

■お問い合わせ先

テクニカルサポートセンター
https://www.contec.com/jp/tsc/