公開日　2026 年 09 月 10 日

株式会社コンテック

当社 FLEXLAN シリーズ製品における脆弱性について

■概要

複数の当社製品において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ならびに対策方法・回避策を製品シリーズごとに示します。対策、軽減または回避策の実施をお願いいたします。

対象製品名一覧

①	無線 LAN FLEXLAN シリーズ	FX5000/FX4000/FX3000 シリーズ
②	無線 LAN FLEXLAN シリーズ	SGA1000
③	無線 LAN FLEXLAN シリーズ	RP-WAH-SR
④	無線 LAN FLEXLAN シリーズ	EC1000 シリーズ

■対象商品①

シリーズ名　：無線LAN FLEXLANシリーズ
製品名　　：FX5000シリーズ、FX4000シリーズ、FX3000シリーズ
製品型式　：FXA5000、FXA5020、FXA5020-□□、FXE5000、FXE5000-□□
FXS5000-□□、FXS5021
FXE4000、FXE4000-WP、FXS4000、FXS4020
FXA3000、FXA3000-□□、FXA3020、FXA3020-□□、FXA3200
FXE3000、FXE3000-□□、FXS300□-CN、FXE3000-WP
バージョン　：FX5000 シリーズ　1.12.00 未満
FX4000 シリーズ　1.14.00 未満
FX3000 シリーズ　1.20.00 未満

・判明した脆弱性と脆弱性がもたらす脅威

① CVE-2026-82762：「FLEXLAN FX5000/4000/3000 シリーズにおける OS コマンドインジェクション」…CWE-78
入力値の検証が適切に実施されておらず、悪意ある攻撃者に利用されることで任意のコマンドを実行され、情報の盗用や改竄、悪意あるプログラムの実行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-2026-82763：「FLEXLAN FX5000/4000/3000 シリーズにおけるクロスサイトスクリプティング」…CWE-79
設定画面にクロスサイトスクリプティングの脆弱性があり、悪意のある攻撃者に利用されることで不正なサイトへの誘導を行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:L / UI:R / S:C / C:L / I:L / A:N　　基本値：5.4

③ CVE-2026-82764：「コンテック製品におけるクロスサイトリクエストフォージェリ」…CWE-352
クロスサイトリクエストフォージェリの脆弱性があり、悪意のある攻撃者に利用されることで不正なサイトへの誘導を行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:N / UI:R / S:U / C:N / I:L / A:N　　基本値：4.3

④ CVE-2026-82765：「FLEXLAN FX5000/4000/3000 シリーズにおけるパストラバーサル」…CWE-23
FTP でアクセスした際にパストラバーサルの脆弱性があり、悪意のある攻撃者に利用されることで情報の盗用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:N　　基本値：8.1

・対策方法

ファームウェアを上記脆弱性の対策を施した最新バージョンに更新してください。
最新のファームウェアは当社 Web サイトより入手できます。
ファームウェアの更新手順につきましては、マニュアルやヘルプなどをご確認ください。

- FX5000 シリーズ（対策済みバージョン：Ver.1.12.00 以降）
https://www.contec.com/jp/products-services/daq-control/flexlan-iot/wlan-module/fxe5000/support/#firmware

- FX4000 シリーズ（対策済みバージョン：Ver.1.14.00 以降）
https://www.contec.com/jp/products-services/daq-control/flexlan-iot/wlan-module/fxe4000/support/#firmware

- FX3000 シリーズ（対策済みバージョン：Ver.1.20.00 以降）
  https://www.contec.com/jp/products-services/daq-control/flexlan-iot/wlan-module/fxe3000/support/#firmware

ダウンロード検索を使用する場合は、以下の検索サイトにアクセスの上、対象製品の型式を入力し、ファームウェアを指定して検索してください。

- 検索サイト
  https://www.contec.com/jp/download/search/

・回避策

対策済み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、当社は以下に示す軽減策を講じることを推奨します。

・本製品にアクセスするためのログインパスワードをデフォルトから変更する
・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し信頼できる通信のみ許可する
・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

■対象商品②

シリーズ名　：無線LAN FLEXLANシリーズ
製品名　　：SGA1000
製品型式　　：SGA1000
バージョン　：1.02 未満

・判明した脆弱性と脆弱性がもたらす脅威

① CVE-2026-82766 :「FLEXLAN SGA1000 における OS コマンドインジェクション」…CWE-78
入力値の検証が適切に実施されておらず、悪意ある攻撃者に利用されることで任意のコマンドを実行され、情報の盗用や改、悪意あるプログラムの実行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-2026-82767 :「FLEXLAN SGA1000 におけるクロスサイトスクリプティング」…CWE-79
設定画面にクロスサイトスクリプティングの脆弱性があり、悪意のある攻撃者に利用されることで不正なサイトへの誘導を行われる可能性があります。
CVSS:3.1 / AV:A / AC:L / PR:N / UI:R / S:C / C:L / I:L / A:N　　基本値：5.2

③ CVE-2026-82764 :「コンテック製品におけるクロスサイトリクエストフォージェリ」…CWE-352
クロスサイトリクエストフォージェリの脆弱性があり、悪意のある攻撃者に利用されることで不正なサイトへの誘導を行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:N / UI:R / S:U / C:N / I:L / A:N　　基本値：4.3

④ CVE-2026-82768 :「FLEXLAN SGA1000 におけるパストラバーサル」…CWE-23
FTP でアクセスした際にパストラバーサルの脆弱性があり、悪意のある攻撃者に利用されることで情報の盗用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:N　　基本値：8.1

・対策方法

ファームウェアを上記脆弱性の対策を施した最新バージョンに更新してください。
最新のファームウェアは当社 Web サイトより入手できます。
ファームウェアの更新手順につきましては、マニュアルやヘルプなどをご確認ください。

- SGA1000（対策済みバージョン：Ver.1.02 以降）
  https://www.contec.com/jp/products-services/computer-networking/flexlan-fx/fx-accesspoint/sga1000/support/#firmware

ダウンロード検索を使用する場合は、以下の検索サイトにアクセスの上、対象製品の型式を入力し、ファームウェアを指定して検索してください。

- 検索サイト
  https://www.contec.com/jp/download/search/

・回避策

対策済み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、当社は以下に示す軽減策を講じることを推奨します。

・本製品をネットワーク回線から切り離す
・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し信頼できる通信のみ許可する
・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

■**対象商品③**

シリーズ名　：無線LAN FLEXLANシリーズ
製品名　　：RP-WAH-SRシリーズ
製品型式　　：RP-WAH-SR1、RP-WAH-SR2、RP-WAH-SR12、RP-WAH-SR22
バージョン　：RP-WAH-SR1、RP-WAH-SR2　　：1.03 未満
　　RP-WAH-SR12、RP-WAH-SR22　：1.02 未満

・判明した脆弱性と脆弱性がもたらす脅威

① CVE-2026-82769：「FLEXLAN RP-WAH-SR におけるクロスサイトスクリプティング」…CWE-79
設定画面にクロスサイトスクリプティングの脆弱性があり、悪意のある攻撃者に利用されることで不正なサイトへの誘導を行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:L / UI:R / S:C / C:L / I:L / A:N　　基本値：5.4

② CVE-2026-82764：「コンテック製品におけるクロスサイトリクエストフォージェリ」…CWE-352
クロスサイトリクエストフォージェリの脆弱性があり、悪意のある攻撃者に利用されることで不正なサイトへの誘導を行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:N / UI:R / S:U / C:N / I:L / A:N　　基本値：4.3

㋐ CVE-2026-82770：「FLEXLAN RP-WAH-SR におけるバッファオーバーフロー」…CWE-120
改竄したバックアップファイルを Web 転送する際にバッファオーバーフローの脆弱性があり、悪意のある攻撃者に利用されることで情報の盗用や改竄、悪意あるプログラムの実行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

・対策方法

ファームウェアを上記脆弱性の対策を施した最新バージョンに更新してください。
最新のファームウェアは当社 Web サイトより入手できます。
ファームウェアの更新手順につきましては、マニュアルやヘルプなどをご確認ください。

- RP-WAH-SR1、RP-WAH-SR2（対策済みバージョン：Ver.1.03 以降）
  https://www.contec.com/jp/products-services/daq-control/flexlan-iot/media-converter/rp-wah-sr1/support/#firmware

- RP-WAH-SR12、RP-WAH-SR22（対策済みバージョン：Ver.1.02 以降）
  https://www.contec.com/jp/products-services/daq-control/flexlan-iot/media-converter/rp-wah-sr12/support/#firmware

ダウンロード検索を使用する場合は、以下の検索サイトにアクセスの上、対象製品の型式を入力し、ファームウェアを指定して検索してください。

- 検索サイト
  https://www.contec.com/jp/download/search/

・回避策

対策済み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、当社は以下に示す軽減策を講じることを推奨します。

・本製品をネットワーク回線から切り離す
・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し信頼できる通信のみ許可する
・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

■対象商品④

シリーズ名　：無線LAN FLEXLANシリーズ
製品名　　：EC1000シリーズ
製品型式　　：ECE1000、ECE1020、ECS1020
バージョン　：1.02 未満

・判明した脆弱性と脆弱性がもたらす脅威

① CVE-2026-82771：「FLEXLAN EC1000 シリーズにおけるクロスサイトスクリプティング」…CWE-79
設定画面にクロスサイトスクリプティングの脆弱性があり、悪意のある攻撃者に利用されることで不正なサイトへの誘導を行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:L / UI:R / S:C / C:L / I:L / A:N　　基本値：5.4

② CVE-2026-82764：「コンテック製品におけるクロスサイトリクエストフォージェリ」…CWE-352
クロスサイトリクエストフォージェリの脆弱性があり、悪意のある攻撃者に利用されることで不正なサイトへの誘導を行われる可能性があります。
CVSS:3.1 / AV:N / AC:L / PR:N / UI:R / S:U / C:N / I:L / A:N　　基本値：4.3

㋐ CVE-2026-82772：「FLEXLAN EC1000 シリーズにおけるバッファオーバーフロー」…CWE-120
改竄したバックアップファイルを Web 転送する際にバッファオーバーフローの脆弱性があり、悪意のある攻撃者に利用されることで情報の盗用や改竄、悪意あるプログラムの実行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

・対策方法

ファームウェアを上記脆弱性の対策を施した最新バージョンに更新してください。
最新のファームウェアは当社 Web サイトより入手できます。
ファームウェアの更新手順につきましては、マニュアルやヘルプなどをご確認ください。

- ECE1000（対策済みバージョン：Ver.1.02 以降）
  https://www.contec.com/jp/products-services/daq-control/flexlan-iot/wlan-module/ece1000/support/#firmware

- ECE1020（対策済みバージョン：Ver.1.02 以降）
  https://www.contec.com/jp/products-services/daq-control/flexlan-iot/wlan-module/ece1020/support/#firmware

- ECS1020（対策済みバージョン：Ver.1.02 以降）
  https://www.contec.com/jp/products-services/daq-control/flexlan-iot/wlan-module/ecs1020/support/#firmware

ダウンロード検索を使用する場合は、以下の検索サイトにアクセスの上、対象製品の型式を入力し、ファームウェアを指定して検索してください。

- 検索サイト
  https://www.contec.com/jp/download/search/

・回避策

対策済み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、当社は以下に示す軽減策を講じることを推奨します。

・本製品をネットワーク回線から切り離す
・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し信頼できる通信のみ許可する
・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

■関連情報

・JVNVU#99009004
https://jvn.jp/vu/JVNVU99009004/

■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/support/technical-support/

■改訂履歴

・2026 年 09 月 10 日　　初版