公開日　2026 年 11 月 06 日

株式会社コンテック

# FLEXLAN シリーズ製品における PHP の脆弱性について

## ■ 概要

The PHP Group から、PHP における 2 件の脆弱性（CVE-2026-109618、CVE-2026-109619）が公開されました。これらの脆弱性が悪用されると、認証されていない遠隔の第三者に、対象システム上で任意のコードを実行される可能性があります。
当社で調査した結果、以下の FLEXLAN シリーズ製品が本脆弱性の影響を受けることを確認しました。対象製品と対応方法を以下に示します。
対象製品を使用している場合は、対策済みバージョンへ更新してください。

### 対象製品名一覧

① 無線 LAN FLEXLAN シリーズ　　SGA1000

■ **対象製品 ①**

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　：1.03 未満

- **判明した脆弱性と脆弱性がもたらす脅威**

① CVE-2026-109618 :「PHP のメモリ不足時の処理に起因する脆弱性」…CWE-416
認証されていない遠隔の第三者により、任意のコードを実行される可能性があります
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
基本値：9.2（The PHP Group の公表）

② CVE-2026-109619 :「PHP の解放済みメモリに関連する内部状態の処理に起因する脆弱性」…CWE-416
認証されていない遠隔の第三者により、任意のコードを実行される可能性があります。
CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
基本値：9.2（The PHP Group の公表）

- **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 サイトから入手できます。
ファームウェアの更新手順については、マニュアルやヘルプを参照してください。

- SGA1000（対策済みバージョン：Ver.1.03 以降）
https://www.contec.com/jp/download/contract/contract2/?itemid=c16128fb-d05d-483a-8dd7-75245d9d7ad7&downloaditemid=fed14cda-fa1e-42a4-8312-08bc26e85ae3

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**

- The PHP Group
https://www.php.net/archive/2026.php#2026-10-21-5
- JVNVU#99905564
https://jvn.jp/vu/JVNVU99905564/

■ **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/

■ **改訂履歴**

2026 年 11 月 06 日　初版