# ネットワークカメラ TRIFORA 3 シリーズにおける複数の脆弱性

公開日：2025 年 10 月 1 日
最終更新日：2025 年 10 月 10 日
TOA 株式会社

■脆弱性情報 ID
TV2025-001

■概要
ネットワークカメラ TRIFORA 3 シリーズにおいて、複数の脆弱性を確認しました。これらの脆弱性により、悪意ある第三者によって任意のコマンド実行や不正なスクリプトの挿入、アクセス制限されたファイルへの不正アクセスが行われる可能性があります。

現時点では、これらの脆弱性を悪用した攻撃の発生は確認されておりませんが、より安心してご使用いただくため、該当製品をご使用中のお客様は修正済みファームウェアへアップデートしていただきますようお願いいたします。

■該当製品の確認方法
影響を受ける製品は以下の通りです。

| 品名 | 品番 | 対象ファームウェアバージョン |
|---|---|---|
| フルＨＤネットワークカメラ | N-C3100-3 | すべてのバージョン |
| フルＨＤネットワークカメラ | N-C3120 | すべてのバージョン |
| フルＨＤネットワークカメラ | N-C3120-3 | すべてのバージョン |
| ドーム型フルＨＤネットワークカメラ | N-C3200-3 | すべてのバージョン |
| ドーム型フルＨＤネットワークカメラ | N-C3220-3 | すべてのバージョン |
| 屋外フルＨＤネットワークカメラ | N-C3420-3 | すべてのバージョン |
| 屋外赤外フルＨＤネットワークカメラ | N-C3420R3 | すべてのバージョン |
| フルＨＤネットワークＰＴＺカメラ | N-C3500 | すべてのバージョン |
| フルＨＤネットワークＰＴＺカメラ | N-C3500A | すべてのバージョン |
| 屋外フルＨＤネットワークＰＴＺカメラ | N-C3700 | すべてのバージョン |
| 屋外フルＨＤネットワークＰＴＺカメラ | N-C3700A | すべてのバージョン |
| 屋外ドーム型フルＨＤネットワークカメラ | N-C3820-3 | すべてのバージョン |

■脆弱性の説明

| 脆弱性種別 | 脆弱性内容 | CVSS スコア |
|---|---|---|
| OS コマンドインジェクション<br>(CWE-78) | 不正な URL を指定することで、任意の OS コマンドが実行される可能性 | CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H<br>基本値：8.0 |
| クロスサイトスクリプティング<br>(CWE-79) | Web ビューアー(設定画面)において不正な値を設定することで、任意のスクリプトが実行される可能性 | CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N<br>基本値：4.3 |
| パストラバーサル<br>(CWE-22) | 不正な URL を指定することで、本来アクセスできないファイルにアクセスされる可能性 | CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N<br>基本値：5.7 |

■対策方法

本脆弱性に対する対策として、該当製品に対して、脆弱性を修正したファームウェアをご提供しております。当社商品データダウンロードサイトから品番を検索して修正済みファームウェアをダウンロードいただき、アップデートを実施してください。

ファームウェアのアップデート方法は、「操作・設定ガイド」の「3-2 メンテナンスのしかた -> メンテナンス -> 機器メンテナンス -> ファームウェアのアップデートをする」をご参照ください。

商品データ ダウンロードサイト

https://www.toa-products.com/download/

修正済みファームウェア

Ver1.3.1 以降

■謝辞

この問題をご報告いただいた GMO サイバーセキュリティ by イエラエ株式会社 井餘田 笙悟 様に感謝いたします。

■お問い合わせ窓口

本件に関するお問い合わせは、当社の各営業所にて承っております。最寄りの当社営業所までお問い合わせください。
https://www.toa-global.com/ja/profile/company/network

■関連情報

JVN#08087148, JVN#02416100, JVN#69025226

■更新履歴

2025 年 10 月 10 日

「概要」欄を修正しました。

2025 年 10 月 1 日

この脆弱性情報を公開しました。