株式会社マイクロリサーチ
セキュリティ脆弱性情報
MR-GM5L-S1/MR-GM5A-L1 製品

JVNVU#98103854: MR-GM5L-S1、MR-GM5A-L1 製品における

複数の脆弱性(ｺｰﾄﾞｲﾝｼﾞｪｸｼｮﾝ/不正ﾛｸﾞｲﾝ/認証回避を伴う RCE)

公開日 2026 年 3 月 11 日

■概要

弊社製品 MR-GM5L-S1/MR-GM5A-L1(以下、MR-GM5 シリーズと略します)用ファームウェア v2.01.04N1_02(2026 年 3 月 11 日公開)より前のファームウェアに複数の脆弱性(コードインジェクション/不正ログイン/認証回避を伴う RCE)が存在することが判明致しました。この脆弱性を悪用された場合、MR-GM5 シリーズ製品への不正ログインや root 権限下で任意コマンドの実行がおこなわれてしまう危険性があります。この問題の影響を受ける MR-GM5 シリーズのファームウェアバージョンを以下に示しますので、修正プログラムを適用してください。

■該当製品の確認方法

影響を受ける製品は以下の製品です。

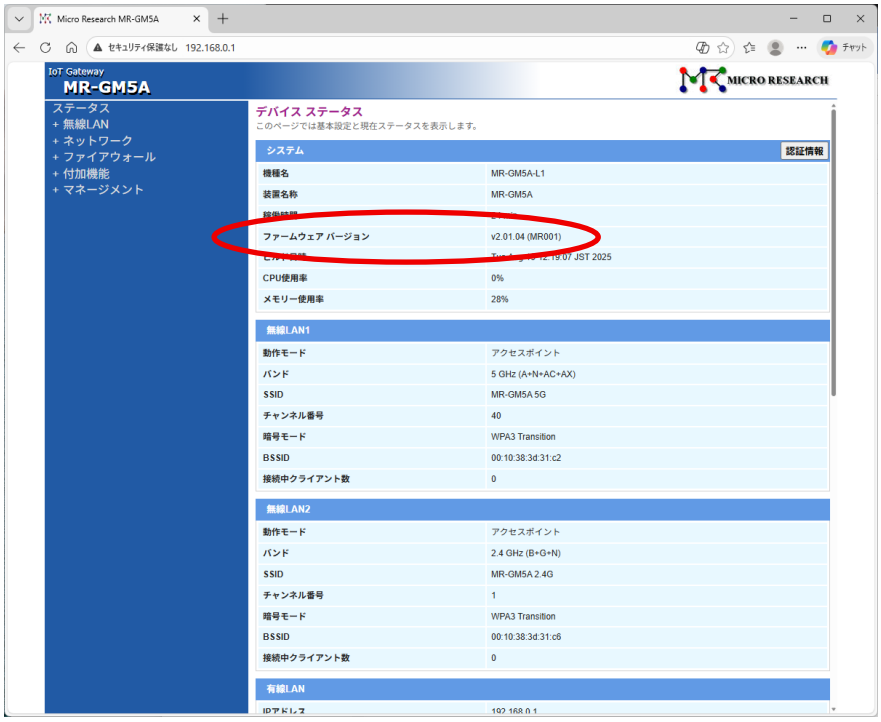
該当製品①
製品名称：MR-GM5L-S1
ファームウェアバージョン：v2.01.04N1_02 より前の全てのファームウェアバージョン
該当製品②
製品名称：MR-GM5A-L1
ファームウェアバージョン：v2.01.04N1_02 より前の全てのファームウェアバージョン

現在動作しているファームウェアバージョンの確認方法は以下の通りです。

1. MR-GM5 シリーズの GUI 設定画面を開き、ステータス画面で「ファームウェアバージョン」の項目を確認します。

<< 次ページへ続く >>

ステータス画面の表示例(MR-GM5A-L1)



■脆弱性の説明

MR-GM5 シリーズにおいて、以下の複数の脆弱性が確認されております。

① root 権限下での任意コードの実行

設定画面ログイン後、意図しない方法により root 権限下で任意のコードが実行されてしまう事を確認しております。

② 認証不備による不正ログイン

弊社の意図しない方法により、設定画面に不正にログインできてしまう事を確認しております。

③ 認証回避を含む root 権限下でのリモートコード実行

認証無しに root 権限下で任意のコードが実行されてしまう事を確認しております。

■脆弱性がもたらす脅威

悪意ある第三者は、脆弱性の説明①、②の組み合わせにより正規ログインを行わないでも root 権限下による任意のコマンドを実行する事が可能です。また、脆弱性の説明③により、root 権限下でのリモートコードの実行が可能です。これにより、MR-GM5 シリーズは、悪意ある第三者のコントロール下におかれ、他システムへの攻撃や破壊行為への踏み台、データ盗用や改ざんなどを実行される可能性があります。

■対策方法

ファームウェアバージョン v2.01.04N1_02 より前の製品を利用されているお客様は、ファームウェアバージョン v2.01.04N1_02 以後のファームウェアをインストールしてください。

■更新履歴

2026 年 3 月 11 日　　このセキュリティ脆弱性情報ページを公開しました。

■連絡先

脆弱性連絡窓口　　電話: 03-3458-9422 (平日 10:00 – 17:00)