SANYO DENKI

H0033413

# SANUPS SOFTWARE STANDALONE/SANUPS SOFTWARE

# 脆弱性に伴うバージョンアップのご案内

2026年3月23日

山洋電気株式会社

エレクトロニクスカンパニー

## 1．概要

当社の無停電電源装置（UPS）用の管理ソフトにおいて、Windowsサービスの実行ファイルパスが引用符で囲まれていない脆弱性（CWE-428）が存在することが判明しました。

本脆弱性の影響を受ける製品と該当バージョンならびに推奨する対策方法をご案内します。

## 2．対象製品と対策方法

該当製品をご使用の場合は、アップデートまたは置換えをお願いします。

| 製品名 | バージョン | 対策方法 |
|---|---|---|
| SANUPS SOFTWARE STANDALONE（※1） | Ver.1.0.1 | Ver1.0.1をアンインストールして、Ver.1.1.5をインストールしてください。（※3）<br>（再設定が必要になります） |
| | Ver.1.1.0～<br>Ver.1.1.4 | Ver.1.1.5へアップデートしてください。（※4）<br>（設定情報は引き継がれます） |
| SANUPS SOFTWARE（※2） | Ver.1.0.0～<br>Ver.1.1.4 | Ver.3.0.1をご購入のうえ、Ver.1.x.xをアンインストールしてから、Ver.3.0.1をインストールしてください。<br>（再設定が必要になります）<br>ただし、Windows2000は対象外です。 |
| | Ver.2.0.0～<br>Ver.2.0.2 | Ver.2.0.3へアップデートしてください。（※5）<br>（設定情報は引き継がれます） |

※1 本案内以前にインストールされたすべてのバージョンが対象です。

※2 現行出荷品（Ver.3.x.x）は本脆弱性の対象外であり、問題ありません。

※3 以下の当社Webサイトからダウンロードしてインストールしてください。
https://products.sanyodenki.com/ja/sanups/software/sanups_software_standalone/

※4 以下の当社Webサイトからダウンロードしてアップデートしてください。
https://products.sanyodenki.com/ja/sanups/software/sanups_software_standalone_updata/

※5 以下の当社Webサイトからダウンロードしてアップデートしてください。
https://products.sanyodenki.com/ja/sanups/software/sanups_software_v2/

## 3．脆弱性の内容

対象製品のインストール先ファルダのパスに空白（スペース）が含まれていると、攻撃者がそのパス上に悪意ある実行ファイルを置くことで、サービス権限で不正プログラムが実行される恐れがあります。

脆弱性（CWE-428）については以下のURLにてご確認ください。

https://jvndb.jvn.jp/ja/cwe/CWE-428.html

## 4．お問い合わせ先

ご不明な点や対応に関するご相談は、下記までご連絡ください。

山洋電気株式会社 エレクトロニクスカンパニー 設計部
UPS 管理ソフト ユーザ係
E-mail sanguard_support@sanyodenki.com

## 5．謝辞

本脆弱性情報は、GMOサイバーセキュリティ byイエラエ株式会社の松本 一真様からご報告いただきました。

脆弱性を発見、ご報告いただいた松本 一真様に感謝申しあげます。

## 6．まとめ

この度はUPS管理ソフトの脆弱性によりご迷惑をおかけしまして誠に申し訳ございません。

今後とも、品質の維持向上に努めてまいりますので、よろしくお願い申しあげます。

以上