SANYO DENKI

H0033413

Date: March 23, 2026

SANYO DENKI CO., LTD.
Electronics Company

Notice of Version Upgrade Due to a Security Vulnerability in SANUPS SOFTWARE STANDALONE and SANUPS SOFTWARE

1. Overview

We have identified a security vulnerability (CWE-428) in our UPS management software, in which the executable path of a Windows service is not enclosed in quotation marks. This notice provides details of the affected products and versions, as well as the recommended countermeasures.

2. Affected Products and Countermeasures

If you are using any of the affected products, please apply an update or replace the software as described below.

Product Name	Version	Countermeasures
SANUPS SOFTWARE STANDALONE[1]	Ver.1.0.1	Uninstall Ver1.0.1 and install Ver.1.1.5.[3] (Reconfiguration will be required.)
	Ver.1.1.0 to Ver.1.1.4	Update to Ver.1.1.5.[4] (Configuration settings will be retained.)
SANUPS SOFTWARE[2]	Ver.1.0.0 to Ver.1.1.4	Purchase Ver.3.0.1, uninstall Ver.1.x.x, and then install Ver.3.0.1. (Reconfiguration will be required.) Note: Windows 2000 is not supported.
	Ver.2.0.0 to Ver.2.0.2	Update to Ver.2.0.3.[5] (Configuration settings will be retained.)

[1] All versions installed prior to the issuance of this notice are affected.

[2] Currently shipped products (Ver. 3.x.x) are not affected by this vulnerability.

[3] Please download and install the software from our website listed below.
https://products.sanyodenki.com/en/sanups/software/sanups_software_standalone/

[4] Please download and install the software from our website listed below.
https://products.sanyodenki.com/ja/sanups/software/sanups_software_standalone_updata/

[5] Please download and install the software from our website listed below.
https://products.sanyodenki.com/ja/sanups/software/sanups_software_v2/

3. Details of the Vulnerability

If the installation path of the affected product contains spaces, an attacker may place a malicious executable in that path, potentially causing unauthorized programs to be executed with service-level privileges.

For more information on this vulnerability (CWE-428), please refer to the following URL.

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

4. Contact Information

If you have any questions or need assistance with the above measures, please contact us at the email address below.

Design Department
UPS Management Software User Support Team
Electronics Company
SANYO DENKI CO., LTD.
E-mail: sanguard_support@sanyodenki.com

5. Acknowledgment

This vulnerability was reported by Mr. Kazuma Matsumoto of GMO Cybersecurity by Ierae, Inc. We would like to express our sincere appreciation for the discovery and responsible disclosure of this issue.

6. Closing

We sincerely apologize for any inconvenience caused by this vulnerability in our UPS management software. We will continue to strive to maintain and improve the quality and security of our products. Thank you for your continued support.