

## **SSA-537983: Local Code Execution Vulnerability in SENTRON powermanager V3**

Publication Date: 2021-11-09  
Last Update: 2021-11-09  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.8

### **SUMMARY**

SENTRON powermanager V3 is affected by a vulnerability that could allow a local attacker to inject arbitrary code and escalate privileges.

Siemens has released a security patch for SENTRON powermanager V3.6 HF1 and recommends to update to the latest version and apply this patch.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
SENTRON powermanager V3: All versions	Update to V3.6 HF1 and apply the security patch <a href="https://support.industry.siemens.com/cs/ww/en/view/64850998/">https://support.industry.siemens.com/cs/ww/en/view/64850998/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

### **WORKAROUNDS AND MITIGATIONS**

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Harden the application server to prevent local access by untrusted personnel

### **GENERAL SECURITY RECOMMENDATIONS**

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: <https://www.siemens.com/cert/operational-guidelines-industrial-security>), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: <https://www.siemens.com/industrialsecurity>

### **PRODUCT DESCRIPTION**

The SENTRON powermanager power monitoring software analyzes energy consumption by displaying important characteristics for individual devices and for the entire system on an easy-to-understand dashboard.

### **VULNERABILITY CLASSIFICATION**

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (<https://www.first.org/cvss/>). The CVSS environmental score is specific to the customer's

environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: <https://cwe.mitre.org/>.

Vulnerability CVE-2021-37207

The affected application assigns improper access rights to a specific folder containing configuration files.

This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C</a>
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

## **ACKNOWLEDGMENTS**

Siemens thanks the following parties for their efforts:

- Noam Moshe from Claroty for coordinated disclosure

## **ADDITIONAL INFORMATION**

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

<https://www.siemens.com/cert/advisories>

## **HISTORY DATA**

V1.0 (2021-11-09): Publication Date

## **TERMS OF USE**

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website ([https://www.siemens.com/terms\\_of\\_use](https://www.siemens.com/terms_of_use), hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.