SSA-655554: Multiple Vulnerabilities in SIMATIC Energy Manager before V7.3 Update 1

Publication Date: 2022-04-12
Last Update: 2022-04-12
Current Version: V1.0
CVSS v3.1 Base Score: 10.0

SUMMARY

SIMATIC Energy Manager is affected by multiple vulnerabilities that could allow an attacker to gain local privilege escalation, local code execution or remote code execution.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Energy Manager Basic: All versions < V7.3 Update 1	Update to V7.3 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109808211/ See further recommendations from section Workarounds and Mitigations
SIMATIC Energy Manager PRO: All versions < V7.3 Update 1	Update to V7.3 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109808211/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to the affected systems, especially to port 4444/tcp, to trusted IP addresses only
- Enable encryption in the SIMATIC Energy Manager configuration

Product specific remediations or mitigations can be found in the section Affected Products and Solution.

Please follow the General Security Recommendations.

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

With SIMATIC Energy Manager, you can visualize energy flows and consumption values in your processes in detail, assign them to the relevant consumers or cost centers, and identify why changes have occurred. Evaluate implemented efficiency measures, optimize your energy procurement, and compare energy efficiency across plants and locations – in a scalable, transparent, and future-proof way.

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-2022-23448

Affected applications improperly assign permissions to critical directories and files used by the application processes. This could allow a local unprivileged attacker to achieve code execution with ADMINISTRATOR or even NT AUTHORITY/SYSTEM privileges.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2022-23449

A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges by placing a malicious DLL in one of the directories on the DLL search path.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-427: Uncontrolled Search Path Element

Vulnerability CVE-2022-23450

The affected system allows remote users to send maliciously crafted objects. Due to insecure deserialization of user-supplied content by the affected software, an unauthenticated attacker could exploit this vulnerability by sending a maliciously crafted serialized object. This could allow the attacker to execute arbitrary code on the device with SYSTEM privileges.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-502: Deserialization of Untrusted Data

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 (2022-04-12): Publication Date

TERMS OF USE