SSA-145157: Multiple Vulnerabilities in SIMATIC RTLS Locating Manager before V2.12

Publication Date: 2021-11-09
Last Update: 2021-11-09
Current Version: V1.0
CVSS v3.1 Base Score: 5.5

SUMMARY

SIMATIC RTLS Locating Manager before V2.12 contains multiple vulnerabilities that could allow an attacker to read sensitive data or trigger a denial-of-service condition of the application service.

Siemens has released an update for the SIMATIC RTLS Locating Manager and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC RTLS Locating Manager: All versions < V2.12	Update to V2.12 or later version https://support.industry.siemens.com/cs/ww/en/view/109803363/ 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:

- Apply security hardening of the Windows Server, where the RTLS Locating Manager is installed on, in accordance with your corporate security policies or up-to-date hardening guidelines
- Ensure that only trusted persons have access to the system and avoid the configuration of additional local accounts on the server

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 SIMATIC RTLS Locating Manager is used for the configuration, operation, and maintenance of a SIMATIC RTLS installation, which is real-time wireless locating system for flexible and cost-effective locating solutions.

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-2020-10052

The affected application writes sensitive data, such as usernames and passwords in log files. A local attacker with access to the log files could use this information to launch further attacks.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-532: Insertion of Sensitive Information into Log File

Vulnerability CVE-2020-10053

The affected application writes sensitive data, such as database credentials in configuration files. A local attacker with access to the configuration files could use this information to launch further attacks.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-312: Cleartext Storage of Sensitive Information

Vulnerability CVE-2020-10054

The affected application does not properly handle the import of large configuration files. A local attacker could import a specially crafted file which could lead to a denial-of-service condition of the application service.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

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