SSA-251935: Multiple Privilege Escalation Vulnerabilities in SIMATIC RTLS Locating Manager

Publication Date: 2020-09-08
Last Update: 2020-09-08
Current Version: V1.0
CVSS v3.1 Base Score: 8.4

SUMMARY

The latest update for SIMATIC RTLS Locating Manager fixes various vulnerabilities that could allow a low-privileged local user to escalate privileges.

Siemens recommends to apply the update of the SIMATIC RTLS Locating Manager.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC RTLS Locating Manager: All versions < V2.10.2	Update to V2.10.2 https://support.industry.siemens.com/cs/ww/en/view/109781166

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

SIMATIC RTLS is a real-time wireless locating system for flexible and cost-effective locating solutions. It allows to navigate material flows, control mobile robots, monitor the use of components, and document the assembly of the end product.

The SIMATIC RTLS Locating Manager is used for the configuration, operation, and maintenance of a SIMATIC RTLS installation.

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-2020-10049

The start-stop scripts for the services of the affected application could allow a local attacker to include arbitrary commands that are executed when services are started or stopped interactively by system administrators.

CVSS v3.1 Base Score	7.9
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-276: Incorrect Default Permissions

Vulnerability CVE-2020-10050

The directory of service executables of the affected application could allow a local attacker to include arbitrary commands that are executed with SYSTEM privileges when the system restarts.

CVSS v3.1 Base Score	8.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-276: Incorrect Default Permissions

Vulnerability CVE-2020-10051

Multiple services of the affected application are executed with SYSTEM privileges while the call path is not quoted. This could allow a local attacker to inject arbitrary commands that are execeuted instead of the legitimate service.

CVSS v3.1 Base Score	8.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-428: Unquoted Search Path or Element

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 (2020-09-08):	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, 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.