SSA-878278: Denial-of-Service Vulnerability in SIMATIC WinAC RTX (F) 2010

Publication Date: 2019-10-08
Last Update: 2020-01-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability in SIMATIC WinAC RTX (F) 2010 controller software could allow an attacker to perform a denial-of-service attack if a large HTTP request is sent to the network port of the host where WinAC RTX is running.

Siemens has released SIMATIC WinAC RTX (F) 2010 incl. SP3 Update 1 that fixes the vulnerability, and recommends that customers update to this new version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinAC RTX (F) 2010: All versions < SP3 Update 1	Update to SIMATIC WinAC RTX (F) 2010 SP3 Update 1 https://support.industry.siemens.com/cs/ww/en/view/109772291

WORKAROUNDS AND MITIGATIONS

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

- Restrict network access to the host containing the affected service.
- If the service is not used as a server, configure Windows Firewall to disable communications on the port of the vulnerable service.

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 WinAC RTX (F) 2010 is a SIMATIC software controller for PC-based automation 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-2019-13921

Affected versions of the software contain a vulnerability that could allow an unauthenticated attacker to trigger a denial-of-service condition. The vulnerability can be triggered if a large HTTP request is sent to the executing service.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the service provided by the software.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CWE	CWE-410: Insufficient Resource Pool

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Tal Keren 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 (2019-10-08):	Publication Date
V1.1 (2020-01-14):	Added update for SIMATIC WinAC RTX (F) 2010

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.