SSA-448291: Denial-of-Service Vulnerability in ARP Protocol of RWG Universal Controllers

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

A Denial-of-Service vulnerability was found affecting the ARP protocol on RWG Universal Controller devices.

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
RWG1.M8: All versions < V1.16.16	Login to the RWG Controller Graphical programming platform, generate a new project file and download the new project file to the device https://www.ubc.siemens.com.cn/
RWG1.M12: All versions < V1.16.16	Login to the RWG Controller Graphical programming platform, generate a new project file and download the new project file to the device https://www.ubc.siemens.com.cn/
RWG1.M12D: All versions < V1.16.16	Login to the RWG Controller Graphical programming platform, generate a new project file and download the new project file to the device https://www.ubc.siemens.com.cn/

WORKAROUNDS AND MITIGATIONS

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

- Ensure that only trusted systems are connected to the same Layer 2 domain as the affected devices
- Restrict access to systems in the same Layer 2 domain as the affected devices to trusted persons only

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

RWG Universal Controllers are used to monitor and control FAU, AHU, heat exchange units, fans, pumps, lighting and other electromechanical equipments.

 © Siemens 2021

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-2021-25671

Sending specially crafted ARP packets to an affected device could cause a partial denial-of-service, preventing the device to operate normally. A restart is needed to restore normal operations.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

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 (2021-07-13): 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.