# SSA-787292: Denial-of-Service Vulnerability in SIMATIC RFID Readers

Publication Date: 2021-06-08
Last Update: 2021-06-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

## SUMMARY

The latest updates for SIMATIC RF products fix a vulnerability that could allow an unauthorized attacker to crash the OPC UA service of the affected devices.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SIMATIC RF166C:<br>All versions > V1.1 and < V1.3.2 | Update to V1.3.2<br>https://support.industry.siemens.com/cs/ww/en/view/109768507 |
| SIMATIC RF185C:<br>All versions > V1.1 and < V1.3.2 | Update to V1.3.2<br>https://support.industry.siemens.com/cs/ww/en/view/109768507 |
| SIMATIC RF186C:<br>All versions > V1.1 and < V1.3.2 | Update to V1.3.2<br>https://support.industry.siemens.com/cs/ww/en/view/109768507 |
| SIMATIC RF186CI:<br>All versions > V1.1 and < V1.3.2 | Update to V1.3.2<br>https://support.industry.siemens.com/cs/ww/en/view/109768507 |
| SIMATIC RF188C:<br>All versions > V1.1 and < V1.3.2 | Update to V1.3.2<br>https://support.industry.siemens.com/cs/ww/en/view/109768507 |
| SIMATIC RF188CI:<br>All versions > V1.1 and < V1.3.2 | Update to V1.3.2<br>https://support.industry.siemens.com/cs/ww/en/view/109768507 |
| SIMATIC RF360R:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC RF615R:<br>All versions > V3.0 | See recommendations from section Workarounds and Mitigations |
| SIMATIC RF680R:<br>All versions > V3.0 | See recommendations from section Workarounds and Mitigations |
| SIMATIC RF685R:<br>All versions > V3.0 | See 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:

- Deactivate the OPC-UA feature of affected devices

## 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 RF185C, RF186C/CI, and RF188C/CI are communication modules for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet and OPC UA.

SIMATIC RF300R is a compact RFID reader for use with Profinet and Ethernet

SIMATIC RF600 Readers are used for the contactless identification of every kind of object, e.g. transport containers, pallets, production goods, or it can be generally used for recording goods in bulk.

## 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-2021-31340

Affected devices do not properly handle large numbers of incoming connections. An attacker may leverage this to cause a Denial-of-Service situation.

| | |
|---|---|
| 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:O/RC:C |
| CWE | CWE-400: Uncontrolled Resource Consumption |

## 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 (2021-06-08): Publication Date

## TERMS OF USE