SSA-288459: Heap Overflow Vulnerability in RFID terminals

Publication Date: 2021-09-14
Last Update: 2021-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.3

SUMMARY

A heap overflow vulnerability in dhclient of the affected products, which has been published alongside other vulnerabilities as part of NAME:WRECK could allow an attacker to potentially remotely execute code.

Siemens recommends specific countermeasures for products.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC RF350M: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF650M: All versions	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:

- Use trusted DNS servers in internal network, and restrict DNS traffic to this network only through firewalls.
- Protect network access to 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 RFx50M are handheld RFID reader/writer terminals with application software for customizing RFID tags.

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-2020-7461

In FreeBSD 12.1-STABLE before r365010, 11.4-STABLE before r365011, 12.1-RELEASE before p9, 11.4-RELEASE before p3, and 11.3-RELEASE before p13, dhclient(8) fails to handle certain malformed input related to handling of DHCP option 119 resulting a heap overflow. The heap overflow could in principle be exploited to achieve remote code execution. The affected process runs with reduced privileges in a Capsicum sandbox, limiting the immediate impact of an exploit.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:U/RC:C
CWE	CWE-787: Out-of-bounds Write

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 (2021-09-14): 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.