SSA-599268: Several Vulnerabilities in TCP Stack of SIMATIC MV400 family

Publication Date: 2021-03-09
Last Update: 2021-03-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

Several vulnerabilities in the TCP stack of the SIMATIC MV400 family could allow an attacker to cause Denial-of-Service condition, or affect integrity of TCP connections.

Siemens has released an update for the SIMATIC MV400 family and recommends to update to the latest version

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC MV400 family: All Versions < V7.0.6	Update to V7.0.6 https://support.industry.siemens.com/cs/ww/en/view/109793481/

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds. Please follow General Security Recommendations.

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

The stationary optical readers of the SIMATIC MV400 family are used to reliably capture printed, lasered, drilled, punched and dotpeen codes on a variety of different surfaces.

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-2020-25241

The underlying TCP stack of the affected products does not correctly validate the sequence number for incoming TCP RST packages. An attacker could exploit this to terminate arbitrary TCP sessions.

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:U/RC:C
CWE	CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input

Vulnerability CVE-2020-27632

ISN generator is initialized with a constant value and has constant increments. An attacker could predict and hijack TCP sessions.

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:H/A:N/E:P/RL:O/RC:C
CWE	CWE-330: Use of Insufficiently Random Values

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 (2021-03-09): 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.