SSA-816980: Multiple Web Vulnerabilities in SIMATIC MV400 Family

Publication Date: 2019-06-11
Last Update: 2021-03-09
Current Version: V1.1
CVSS v3.1 Base Score: 7.1

SUMMARY

The SIMATIC MV400 product family is affected by two web vulnerabilities. The vulnerabilities could allow an authenticated user to escalate privileges, or might expose sensitive information to an attacker that is able to eavesdrop the communication.

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

- By setting the DISA bit, changes to the project by logged-in users can be prevented. Please refer to the Operating Instructions for more details: https://support.industry.siemens.com/cs/ww/en/view/84553392
- 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

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-2019-10925

An authenticated attacker could escalate privileges by sending specially crafted requests to the integrated webserver.

The security vulnerability can be exploited by an attacker with network access to the device. Valid user credentials, but no user interaction are required. Successful exploitation compromises integrity and availability of the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2019-10926

Communication with the device is not encrypted. Data transmitted between the device and the user can be obtained by an attacker in a privileged network position.

The security vulnerability can be exploited by an attacker in a privileged network position which allows eavesdropping the communication between the affected device and the user. The user must invoke a session. Successful exploitation of the vulnerability compromises confidentiality of the data transmitted.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

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 (2019-06-11): Publication Date
V1.1 (2021-03-09): Added update information for MV400

TERMS OF USE