

SSA-816980: Multiple Web Vulnerabilities in SIMATIC Ident MV420 and MV440 families

Publication Date: 2019-06-11
Last Update: 2019-06-11
Current Version: V1.0
CVSS v3.0 Base Score: 7.1

SUMMARY

The SIMATIC Ident MV420 and MV440 families are 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 provides mitigations.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Ident MV420 family: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Ident MV440 family: 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:

- 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/us/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 (<https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf>), 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 Ident families can reliably capture printed, lasered, drilled, punched and dot-peen codes on a variety of different surfaces.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (<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.

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 v3.0 Base Score	7.1
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L/E:P/RL:U/RC:C

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.

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

CVSS v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C

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

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.