SSA-348662: Multiple Vulnerabilities in SIMATIC MV500 Devices before V3.3

Publication Date: 2022-07-12
Last Update: 2022-07-12
Current Version: V1.0
CVSS v3.1 Base Score: 8.0

SUMMARY

SIMATIC MV500 devices before V3.3 are affected by multiple vulnerabilities that could allow attackers to hijack other users' web based management sessions (CVE-2022-33137) or access data on the device without prior authentication (CVE-2022-33138).

Siemens has released an update for the SIMATIC MV500 devices and recommends to update to the latest version. Note that the update also contains additional fixes for vulnerabilities documented in Siemens Security Advisory SSA-712929.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC MV540 H (6GF3540-0GE10): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV540 S (6GF3540-0CD10): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV550 H (6GF3550-0GE10): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV550 S (6GF3550-0CD10): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV560 U (6GF3560-0LE10): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/
SIMATIC MV560 X (6GF3560-0HE10): All versions < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109811878/

WORKAROUNDS AND MITIGATIONS

Product specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the 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

SIMATIC MV500 products are stationary optical readers, 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-2022-33137

The web session management of affected devices does not invalidate session ids in certain logout scenarios. This could allow an authenticated remote attacker to hijack other users' sessions.

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-613: Insufficient Session Expiration

Vulnerability CVE-2022-33138

Affected devices do not perform authentication for several web API endpoints. This could allow an unauthenticated remote attacker to read and download data from the device.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

ADDITIONAL INFORMATION

The update of SIMATIC MV500 devices to V3.3 also contains additional fixes for vulnerabilities documented in the following Siemens Security Advisory:

- SSA-712929 (https://cert-portal.siemens.com/productcert/html/ssa-712929.html)

Refer to the corresponding link for further details.

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 (2022-07-12): Publication Date

TERMS OF USE