SSA-589975 Improper Access Control Vulnerability in CoreShield OWG Software

Publication Date: 2022-09-13
Last Update: 2022-09-13
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

The default installation of the Windows version of the CoreShield One-Way Gateway (OWG) software sets insecure file permissions that could allow a local attacker to escalate privileges to local administrator.

Siemens Mobility has released an update for the CoreShield OWG software and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
CoreShield One-Way Gateway (OWG) Software: All versions < V2.2	Update to V2.2 or later version Contact your Siemens Mobility customer service organization to obtain the update See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Install CoreShield OWG software on a dedicated machine
- Migrate the operating system (OS) of the affected machines to Linux
- Remove modify and write permissions from installed executables for local users

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 Mobility strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

The CoreShield One-Way Gateway (OWG) software enables unidirectional exchange of information between network zones of varying levels of security.

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-2022-38466

The default installation sets insecure file permissions that could allow a local attacker to escalate privileges to local administrator.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

ACKNOWLEDGMENTS

Siemens Mobility thanks the following parties for their efforts:

- Abian Blome and Michael Messner from Siemens Energy for reporting the vulnerability

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens Mobility products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2022-09-13): Publication Date

TERMS OF USE