SSA-536315: Privilege escalation vulnerability in DIGSI 4

Publication Date: 2021-02-09
Last Update: 2021-02-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

A vertical privilege escalation vulnerability exists in DIGSI 4.

Siemens has released an update for DIGSI 4 and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
DIGSI 4: All versions < V4.94 SP1 HF 1	Update to V4.94 SP1 HF 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109740982/

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

DIGSI 4 is the operation and configuration software for SIPROTEC 4 and SIPROTEC Compact protection devices.

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-2020-25245

Several folders in the %PATH% are writeable by normal users. As these folders are included in the search for dlls, an attacker could place dlls there with code executed by SYSTEM.

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-276: Incorrect Default Permissions

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Richard Davy from ECSC Group for coordinated disclosure

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 (2021-02-09): Publication Date

TERMS OF USE