SSA-534283: Insecure File Share Vulnerability in SIMATIC Virtualization as a Service (SIVaaS)

Publication Date: 2025-09-09
Last Update: 2025-09-09
Current Version: V1.0
CVSS v3.1 Base Score: 9.1
CVSS v4.0 Base Score: 9.3

SUMMARY

SIMATIC Virtualization as a Service (SIVaaS) is affected by a vulnerability which exposes a network share without any authentication. This could allow an attacker to access or alter sensitive data without proper authorization.

Siemens recommends to contact technical support to fix the vulnerability.

KNOWN AFFECTED PRODUCTS

Affected Product and Versions	Remediation
SIMATIC Virtualization as a Service (SIVaaS): All versions affected by CVE-2025-40804	Contact Technical Support for assistance

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Known Affected Products. 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 Virtualization as a Service (SiVaaS) enables centralized virtualization of automation systems, providing secure OT/IT integration and standardized industrial monitoring in a robust, scalable environment.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2025-40804

The affected application exposes a network share without any authentication. This could allow an attacker to access or alter sensitive data without proper authorization.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
CVSS v4.0 Base Score	9.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Tim Dijkman from Powerspex for coordinated disclosure

ADDITIONAL INFORMATION

Please contact the Technical support for the below affected MLFB's :

- 9LA1110-6SV40-5DA3
- 9LA1110-6SV40-5FA3
- 9LA1110-6SV40-5FB3
- 9LA1110-6SV40-5FC3
- 9LA1110-6SV40-5JA2
- 9LA1110-6SV40-5XA2
- 9LA1110-6SV40-5XA3

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 (2025-09-09): Publication Date

TERMS OF USE