SSA-997732: Modfem File Parsing Vulnerability in Simcenter Femap before V2021.2

Publication Date:	2021-09-14
Last Update:	2021-09-14
Current Version:	V1.0
CVSS v3.1 Base Score:	3.3

SUMMARY

Siemens Simcenter Femap is affected by a vulnerability that could be triggered when the application reads modfem files. If a user is tricked to open a malicious file with the affected application, an attacker could leverage this vulnerability to leak information in the context of the current process.

Siemens recommends to update to the latest version line of Simcenter Femap (2021.2), which is not affected by this type of vulnerabilities. Siemens recommends to avoid opening of untrusted files from unknown sources.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Simcenter Femap V2020.2: All versions	Update to V2021.2 or later version https://support.sw.siemens.com/ (login required)
Simcenter Femap V2021.1: All versions	Update to V2021.2 or later version https://support.sw.siemens.com/ (login required)

WORKAROUNDS AND MITIGATIONS

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

- Do not open untrusted modfem files from unknown sources

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

Simcenter Femap is an advanced simulation application for creating, editing, and inspecting finite element models of complex products or systems.

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-2021-37176

The femap.exe application lacks proper validation of user-supplied data when parsing modfem files. This could result in an out of bounds read past the end of an allocated buffer.

An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-14260)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure

ADDITIONAL INFORMATION

The latest version line V2021.2 of Simcenter Femap introduces a data integrity for all model data which prevents from similar, yet unknown vulnerabilities of the same category. For compatibility reasons with old model data, this cannot be backported to earlier version lines. Therefore, Siemens encourages to update to this new version line.

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 (2021-09-14):	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.