

SSA-133038: Multiple Modfem File Parsing Vulnerabilities in Simcenter Femap

Publication Date: 2021-06-08
Last Update: 2021-06-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens Simcenter Femap is affected by two vulnerabilities that could be triggered when the application reads modfem files. If a user is tricked to open a malicious file with the affected application, this could lead to a crash, and potentially also to arbitrary code execution or data extraction on the target host system.

Siemens has released updates for Simcenter Femap and recommends to update to the latest version to fix the vulnerabilities. Siemens recommends to avoid opening of untrusted files from unknown sources.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Simcenter Femap 2020.2: All versions < V2020.2.MP3	Update to V2020.2.MP3 or later version https://support.sw.siemens.com/ (login required)
Simcenter Femap 2021.1: All versions < V2021.1.MP3	Update to V2021.1.MP3 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-2021-27387

The femap.exe application lacks proper validation of user-supplied data when parsing FEMAP files. This could result in an out of bounds write past the end of an allocated structure, a different vulnerability than CVE-2021-27399.

An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12819)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-27399

The femap.exe application lacks proper validation of user-supplied data when parsing FEMAP files. This could result in an out of bounds write past the end of an allocated structure, a different vulnerability than CVE-2021-27387.

An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12820)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative 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 (2021-06-08): 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.