

SSA-243317 File Parsing Vulnerability in Simcenter Femap and Parasolid

Publication Date: 2022-07-12
 Last Update: 2022-09-13
 Current Version: V1.2
 CVSS v3.1 Base Score: 7.8

SUMMARY

Simcenter Femap and Parasolid are affected by an out of bounds read vulnerability that could be triggered when the application reads files in NEU format. If a user is tricked to open a malicious file with the affected applications, an attacker could leverage the vulnerability to perform remote code execution in the context of the current process.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Parasolid V33.1: All versions < V33.1.264	Update to V33.1.264 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Parasolid V34.0: All versions < V34.0.250	Update to V34.0.250 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Parasolid V34.1: All versions < V34.1.233	Update to V34.1.233 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Simcenter Femap V2022.1: All versions < V2022.1.3	Update to V2022.1.3 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Simcenter Femap V2022.2: All versions < V2022.2.2	Update to V2022.2.2 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Do not open untrusted NEU files in Simcenter Femap or Parasolid

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 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

Parasolid is a 3D geometric modeling tool that supports various techniques, including solid modeling, direct editing, and free-form surface/sheet modeling.

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-2022-34465

The affected application contains an out of bounds read past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15420)

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-125: Out-of-bounds Read

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 (2022-07-12): Publication Date
V1.1 (2022-08-09): Added fix for Parasolid version line V33.1
V1.2 (2022-09-13): Added fix for Simcenter Femap version lines V2022.1 and V2022.2

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.