

## **SSA-998762: File Parsing Vulnerabilities in Simcenter Femap before V2022.1.2**

Publication Date: 2022-04-12  
Last Update: 2022-04-12  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.8

### **SUMMARY**

Siemens Simcenter Femap versions before V2022.1.2 are affected by vulnerabilities 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 application, an attacker could leverage the vulnerability to leak information or potentially perform remote code execution in the context of the current process.

Siemens recommends to update to the latest version line of Simcenter Femap and to avoid opening of untrusted files from unknown sources.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
Simcenter Femap: All versions < V2022.1.2	Update to V2022.1.2 or later version <a href="https://support.sw.siemens.com/">https://support.sw.siemens.com/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

### **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

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**

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-2022-28661

The affected application contains an out of bounds read past the end of an allocated buffer while parsing specially crafted .NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15114)

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">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</a>
CWE	CWE-125: Out-of-bounds Read

### Vulnerability CVE-2022-28662

The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted .NEU files. This could allow an attacker to leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-15307)

CVSS v3.1 Base Score	3.3
CVSS Vector	<a href="#">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</a>
CWE	CWE-787: Out-of-bounds Write

### Vulnerability CVE-2022-28663

The affected application contains an out of bounds write 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-15592)

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">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</a>
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 (2022-04-12): 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](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.