SSA-609880: File Parsing Vulnerabilities in Simcenter Femap before V2022.1

Publication Date: 2022-02-08
Last Update: 2022-02-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens Simcenter Femap is affected by multiple 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

Affected Product and Versions	Remediation
Simcenter Femap V2020.2: All versions	Update to V2022.1 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
Simcenter Femap V2021.1: All versions	Update to V2022.1 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

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-2021-46151

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-14754, ZDI-CAN-15082)

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-2021-46152

Affected application contains a type confusion vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14643, ZDI-CAN-14644, ZDI-CAN-14755, ZDI-CAN-15183)

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-843: Access of Resource Using Incompatible Type ('Type Confusion')

Vulnerability CVE-2021-46153

Affected application contains a memory corruption vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14645, ZDI-CAN-15305, ZDI-CAN-15589, ZDI-CAN-15599)

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-46154

Affected application contains a stack based buffer overflow vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14646, ZDI-CAN-14679, ZDI-CAN-15084, ZDI-CAN-15304)

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-121: Stack-based Buffer Overflow

Vulnerability CVE-2021-46155

Affected application contains a stack based buffer overflow vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14683, ZDI-CAN-15283, ZDI-CAN-15303, ZDI-CAN-15593)

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-121: Stack-based Buffer Overflow

Vulnerability CVE-2021-46156

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-14684)

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-2021-46157

Affected application contains a memory corruption vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14757)

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-46158

Affected application contains a stack based buffer overflow vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15085, ZDI-CAN-15289, ZDI-CAN-15602)

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-121: Stack-based Buffer Overflow

Vulnerability CVE-2021-46159

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-15050)

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-2021-46160

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-15286)

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-2021-46161

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-15302)

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 (2022-02-08): Publication Date

TERMS OF USE