SSA-064222: Multiple File Parsing Vulnerabilities in Simcenter Femap before V2406

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 7.3

SUMMARY

Simcenter Femap contains multiple file parsing vulnerabilities that could be triggered when the application reads files in IGS, BDF or BMP file formats. If a user is tricked to open a malicious file with any of the affected products, this could lead the application to crash or potentially lead to arbitrary code execution.

Siemens has released a new version for Simcenter Femap and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Simcenter Femap: All versions < V2406 affected by all CVEs	Update to V2406 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:

- CVE-2024-32055, CVE-2024-32056, CVE-2024-32057, CVE-2024-32058, CVE-2024-32059, CVE-2024-32060, CVE-2024-32061, CVE-2024-32062, CVE-2024-32063, CVE-2024-32064, CVE-2024-32065, CVE-2024-32066: Do not open untrusted IGS files in the affected applications
- CVE-2024-33577: Do not open untrusted BDF files in the affected applications
- CVE-2024-33653, CVE-2024-33654: Do not open untrusted BMP files in the affected applications
- Do not open untrusted IGS, BDF or BMP files from using 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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-32055

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process.

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-32056

The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS part file. This could allow an attacker to execute code in the context of the current process.

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2024-32057

The affected application contains a type confusion vulnerability while parsing IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21562)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

Vulnerability CVE-2024-32058

The affected application is vulnerable to memory corruption while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21563)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2024-32059

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21564)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-32060

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21565)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-32061

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21566)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-32062

The affected application contains a type confusion vulnerability while parsing IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21568)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

Vulnerability CVE-2024-32063

The affected application contains a type confusion vulnerability while parsing IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21573)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

Vulnerability CVE-2024-32064

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21575)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-32065

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21577)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-32066

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21578)

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-33577

The affected applications contain a stack overflow vulnerability while parsing specially strings as argument for one of the application binaries. This could allow an attacker to execute code in the context of the current process.

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2024-33653

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2024-33654

The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.

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
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Heinzl for coordinated disclosure of CVE-2024-32055, CVE-2024-32056, CVE-2024-33577, CVE-2024-33653 and CVE-2024-33654
- Trend Micro Zero Day Initiative for coordinated disclosure of vulnerabilities from CVE-2024-32057 through CVE-2024-32066

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 (2024-07-09): 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.