Heap-based buffer overflow in Siemens Simcenter Femap

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-12659
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 14:16:49 UTC
Updated	2026-05-12 14:20:56 UTC
Description	The affected applications contains a memory corruption vulnerability while parsing specially crafted IPT files. This could allc

Risk And Classification

Primary CVSS: v4.0 7.3 HIGH from ics-cert@hq.dhs.gov

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-122 | CWE-122 CWE-122 Heap-based buffer overflow

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	7.3	HIGH	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/E:X/
4.0	CNA	CVSS	7.3	HIGH	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

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

High

ntegrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Siemens	Simcenter Femap	affected V2512.0003 custom	Not specified

References

Reference	Source	Link	Tags
cert-portal.siemens.com/productcert/html/ssa-870926.html	ics-cert@hq.dhs.gov	cert-portal.siemens.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Siemens thanks the following party for its efforts: TrendAI Zero Day Initiative for coordinated disclosure (en)

Additional Advisory Data

Solutions

CNA: Update to V2512.0003 or later version
https://support.sw.siemens.com/product/275652363/

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**