Severity

High

Analysis Summary

CVE-2022-27653 CVSS:7.8

Siemens Simcenter Femap could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write when parsing NEU files. By persuading a victim to open a specially-crafted NEU file, an attacker could exploit this vulnerability to execute arbitrary code on the system.

Impact

- Code Execution

Indicators Of Compromise

CVE

- CVE-2022-27653

Affected Vendors

- Siemens

Affected Products

- Siemens Simcenter Femap 2022.1.1
- Siemens Simcenter Femap 2022.1

Remediation

Refer to Siemens Security Advisory for patch, upgrade or suggested workaround information.

Siemens Security Advisory