

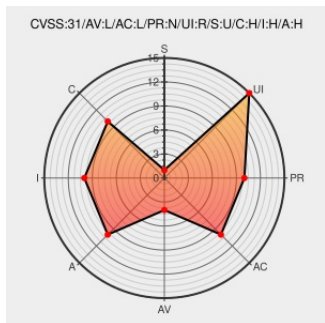


# CVE-2021-27399

Published on: 06/08/2021 12:00:00 AM UTC

Last Modified on: 12/02/2021 01:50:00 PM UTC

## CVE-2021-27399

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Simcenter Femap](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in Simcenter Femap 2020.2 (All versions < V2020.2.MP3), Simcenter Femap 2021.1 (All versions < V2021.1.MP3). The femap.exe application lacks proper validation of user-supplied data when parsing FEMAP files. This could result in an out of bounds write past the end of an allocated structure, a different vulnerability than CVE-2021-27387. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12820)

CVE-2021-27399 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [S](#) **Siemens - Simcenter Femap 2020.2** version **All versions < V2020.2.MP3**

Affected Vendor/Software: [S](#) **Siemens - Simcenter Femap 2021.1** version **All versions < V2021.1.MP3**

CVSS3 Score: **7.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

CVE References

| Description                      | Tags                                                                                                     | Link                                                                                                                                                                                                                      |
|----------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ZDI-21-781   Zero Day Initiative | <a href="http://www.zerodayinitiative.com/text/html">www.zerodayinitiative.com<br/>text/html</a>         |  MISC <a href="http://www.zerodayinitiative.com/advisories/ZDI-21-781/">www.zerodayinitiative.com/advisories/ZDI-21-781/</a>             |
|                                  | <a href="http://cert-portal.siemens.com/application/pdf">cert-portal.siemens.com<br/>application/pdf</a> |  MISC <a href="http://cert-portal.siemens.com/productcert/pdf/ssa-133038.pdf">cert-portal.siemens.com/productcert/pdf/ssa-133038.pdf</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                              | Vendor                  | Product                         | Version | Update            | Edition | Language |
|-------------------------------------------------------------------|-------------------------|---------------------------------|---------|-------------------|---------|----------|
| Application                                                       | <a href="#">Siemens</a> | <a href="#">Simcenter Femap</a> | All     | All               | All     | All      |
| Application                                                       | <a href="#">Siemens</a> | <a href="#">Simcenter Femap</a> | 2020.2  | -                 | All     | All      |
| Application                                                       | <a href="#">Siemens</a> | <a href="#">Simcenter Femap</a> | 2020.2  | maintenance_pack1 | All     | All      |
| Application                                                       | <a href="#">Siemens</a> | <a href="#">Simcenter Femap</a> | 2020.2  | maintenance_pack2 | All     | All      |
| Application                                                       | <a href="#">Siemens</a> | <a href="#">Simcenter Femap</a> | 2021.1  | -                 | All     | All      |
| Application                                                       | <a href="#">Siemens</a> | <a href="#">Simcenter Femap</a> | 2021.1  | maintenance_pack1 | All     | All      |
| Application                                                       | <a href="#">Siemens</a> | <a href="#">Simcenter Femap</a> | 2021.1  | maintenance_pack2 | All     | All      |
| cpe:2.3:a:siemens:simcenter_femap:*****:                          |                         |                                 |         |                   |         |          |
| cpe:2.3:a:siemens:simcenter_femap:2020.2:-:*****:                 |                         |                                 |         |                   |         |          |
| cpe:2.3:a:siemens:simcenter_femap:2020.2:maintenance_pack1:*****: |                         |                                 |         |                   |         |          |
| cpe:2.3:a:siemens:simcenter_femap:2020.2:maintenance_pack2:*****: |                         |                                 |         |                   |         |          |
| cpe:2.3:a:siemens:simcenter_femap:2021.1:-:*****:                 |                         |                                 |         |                   |         |          |
| cpe:2.3:a:siemens:simcenter_femap:2021.1:maintenance_pack1:*****: |                         |                                 |         |                   |         |          |
| cpe:2.3:a:siemens:simcenter_femap:2021.1:maintenance_pack2:*****: |                         |                                 |         |                   |         |          |

No vendor comments have been submitted for this CVE

Social Mentions

| Source                                                                                        | Title                                                                                                                                                                                                   | Posted (UTC)        |
|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @CVEreport | CVE-2021-27399 : A vulnerability has been identified in Simcenter Femap 2020.2 All versions < V2020.2.MP3 , Simcen... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2021-06-08 19:57:25 |
|  /r/netcve  | <a href="#">CVE-2021-27399</a>                                                                                                                                                                          | 2021-06-08          |

[← Previous ID](#)[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)