



# CVE-2021-26597

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-26597  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2021-03-25 19:15:00 UTC   |
| <b>Updated</b>         | 2021-04-01 14:19:00 UTC   |
| <b>Description</b>     | An issue was discovered in Nokia NetAct 18A. A remote user, authenticated to the NOKIA NetAct Web Page, can visit the |

## Risk And Classification

**Problem Types:** CWE-434

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Nokia  | Netact  | 18a     | All    | All     | All      |

## References

| Reference  | Source  | Link   | Tags                |
|--|---------|--|---------------------|
| Trusted Introducer : Directory : Nokia PSIRT                             | MISC    | <a href="http://www.trusted-introducer.org">www.trusted-introducer.org</a> |                     |
| <a href="http://www.gruppettim.it/redteam">www.gruppettim.it/redteam</a> | MISC    | <a href="http://www.gruppettim.it">www.gruppettim.it</a>                   |                     |
| CVE Program record   | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                               | canonical           |
| NVD vulnerability detail   | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                             | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

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](#)**