# CVE Detail – CVE-2022-3979

A vulnerability was found in NagVis up to 1.9.33 and classified as problematic. This issue affects the function checkAuthCookie of the file share/server/core/classes/CoreLogonMultisite.php. The manipulation of the argument hash leads to incorrect type conversion. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 1.9.34 is able to address this issue. The identifier of the patch is 7574fd8a2903282c2e0d1feef5c4876763db21d5. It is recommended to upgrade the affected component. The identifier VDB-213557 was assigned to this vulnerability.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.14338

## CVSS Scoring

CVSS v3.1 Score: 5.6

Severity: MEDIUM

## Mapped CWE(s)

* CWE-704: Incorrect Type Conversion or Cast

## Affected Products

* cpe:2.3:a:nagvis:nagvis:\*:\*:\*:\*:\*:\*:\*:\*