



CVE-2022-3979

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-3979
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-13 23:15:00 UTC
Updated	2023-11-16 03:10:00 UTC
Description	A vulnerability was found in NagVis up to 1.9.33 and classified as problematic. This issue affects the function checkAuthCo

Risk And Classification

Problem Types: CWE-704

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nagvis	Nagvis	All	All	All	All

References

Reference	Source	Link	Tags
Login required	MISC	vuldb.com	
CVE-2022-3979 NagVis CoreLogonMultisite.php checkAuthCookie type conversion	MISC	vuldb.com	
Release nagvis-1.9.34 · NagVis/nagvis · GitHub	MISC	github.com	
Checkmk: Remote Code Execution by Chaining Multiple Bugs (2/3) Sonar	MISC	www.sonarsource.com	
Fix type juggling vulnerability · NagVis/nagvis@7574fd8 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[182234](#) Debian Security Update for nagvis (CVE-2022-3979)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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