



CVE-2023-33477

Published on: Not Yet Published

Last Modified on: 06/13/2023 07:14:00 PM UTC

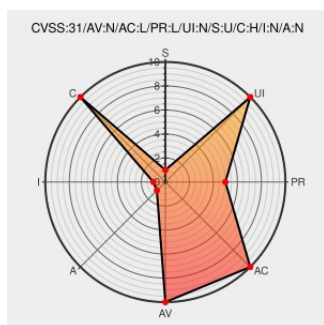
CVE-2023-33477

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Nsg 9000-6g** from **Harmonicinc** contain the following vulnerability:

In Harmonic NSG 9000-6G devices, an authenticated remote user can obtain source code by directly requesting a special path.

CVE-2023-33477 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
GitHub - Skr11lex/CVE-2023-33477	github.com text/html	MISC github.com/Skr11lex/CVE-2023-33477

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Hardware 	Harmonicinc	Nsg 9000-6g	-	All	All	All
Operating System	Harmonicinc	Nsg 9000-6g Firmware	-	All	All	All
cpe:2.3:h:harmonicinc:nsg_9000-6g:-:*:*:*:*:*:						
cpe:2.3:o:harmonicinc:nsg_9000-6g_firmware:-:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
← Previous ID			Next ID→			