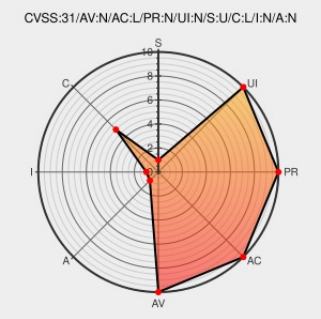
CVE-2023-26126

Published on: Not Yet Published

Last Modified on: 05/16/2023 06:49:00 PM UTC

CVE-2023-26126

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of M.static from M.static Project contain the following vulnerability:

All versions of the package m.static are vulnerable to Directory Traversal due to improper input sanitization of the path being requested via the requestFile function.

CVE-2023-26126 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVE References

Description	Tags	Link
Path traversal vulnerability in m.static@2.2.0 · GitHub	gist.github.com text/html	MISC gist.github.com/lirantal/dcb32c11ce87f5aafd2282b90b4dc998
Directory Traversal in m.static | CVE-2023-26126 | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-MSTATIC-3244915

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	M.static Project	M.static	All	All	All	All

cpe:2.3:a:m.static_project:m.static:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→