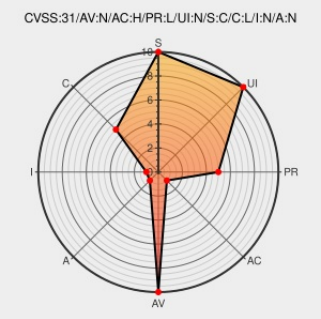
CVE-2021-21298

Published on: 02/26/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:57 PM UTC

CVE-2021-21298 - advisory for GHSA-m33v-338h-4v9f

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



Certain versions of Node-red from Nodered contain the following vulnerability:

Node-Red is a low-code programming for event-driven applications built using nodejs. Node-RED 1.2.7 and earlier has a vulnerability which allows arbitrary path traversal via the Projects API. If the Projects feature is enabled, a user with `projects.read` permission is able to access any file via the Projects API. The issue has been patched in Node-RED 1.2.8. The vulnerability applies only to the Projects feature which is not enabled by default in Node-RED. The primary workaround is not give untrusted users read access to the Node-RED editor.

CVE-2021-21298 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **node-red** - **node-red** version **< 1.2.8**

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Release 1.2.8: Maintenance Release · node-red/node-red · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/node-red/node-red/releases/tag/1.2.8
Restrict project file access to inside the project directory · node-red/node-red@74db3e1 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/node-red/node-red/commit/74db3e17d075f23d9c95d7871586cf461524c456
@node-red/runtime - npm	Product www.npmjs.com text/html	MISC www.npmjs.com/package/@node-red/runtime
Path traversal via Projects API · Advisory · node-red/node-red · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/node-red/node-red/security/advisories/GHSA-m33v-338h-4v9f

Related QID Numbers

982935 Nodejs (npm) Security Update for @node-red/runtime (GHSA-m33v-338h-4v9f)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nodered	Node-red	All	All	All	All
Application	Nodered	Node-red	All	All	All	All

cpe:2.3:a:nodered:node-red:*:*:*:*:*:node.js:*:*

cpe:2.3:a:nodered:node-red:*:*:*:*:*:node.js:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→