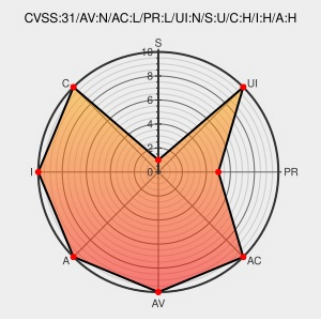
CVE-2023-31874

Published on: Not Yet Published

Last Modified on: 06/03/2023 04:09:00 AM UTC

CVE-2023-31874

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



Certain versions of Yank Note from Yank-note contain the following vulnerability:

Yank Note (YN) 3.52.1 allows execution of arbitrary code when a crafted file is opened, e.g., via nodeRequire('child_process').

CVE-2023-31874 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
Yank Note 3.52.1 Arbitrary Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/172535/Yank-Note-3.52.1-Arbitrary-Code-Execution.html

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

Application	Yank-note	Yank Note	3.52.1	All	All	All

cpe:2.3:a:yank-note:yank_note:3.52.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→