

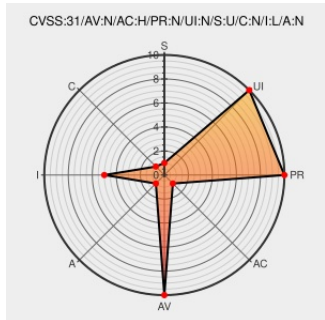


CVE-2023-30857

Published on: Not Yet Published

Last Modified on: 05/08/2023 05:29:00 PM UTC

CVE-2023-30857 - advisory for GHSA-wwxh-74fx-33c6

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [lon](#) from [Aedart](#) contain the following vulnerability:

[@aedart/support](#) is the support package for [lon](#), a monorepo for JavaScript/TypeScript packages. Prior to version `0.6.1`, there is a possible prototype pollution issue for the `MetadataRecord`, when merged with a base class' metadata object, in `meta` decorator from the `@aedart/support` package. The likelihood of exploitation is questionable, given that a class's metadata can only be set or altered when the class is decorated via `meta()`. Furthermore, object(s) of sensitive nature would have to be stored as metadata, before this can lead to a security impact. The issue has been patched in version `0.6.1`.

CVE-2023-30857 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **LOW** severity.

Affected Vendor/Software: [aedart](#) - [lon](#) version = < 0.6.1

CVSS3 Score: **3.7 - LOW**

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

CVE References

Description	Tags	Link
Possible prototype pollution in metadata record, when using meta decorator · Advisory · aedart/ion · GitHub	github.com text/html	MISC github.com/aedart/ion/security/advisories/GHSA-wwxh-74fx-33c6
Fix possible prototype pollution · aedart/ion@c3e2ee0 · GitHub	github.com text/html	MISC github.com/aedart/ion/commit/c3e2ee08710d4164d796ecb66ed291335dae9291

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	Aedart	lon	All	All	All	All
cpe:2.3:a:aedart:lon:*:*:*:*:node.js:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-30857 : @aedart/support is the support package for lon, a monorepo for JavaScript/TypeScript packages. Pri... twitter.com/i/web/status/1...	2023-04-28 21:06:48
 @threatmeter	CVE-2023-30857 aedart support up to 0.6.0 meta MetadataRecord prototype pollution (GHSA-wwwh-74fx-33c6) A vulnera... twitter.com/i/web/status/1...	2023-04-29 07:50:52
 @RedPacketSec	Node.js @aedart/support module security bypass CVE-2023-30857 - redpacketsecurity.com/node-js-aedart... #CVE #Vulnerability #OSINT #ThreatIntel #Cyber	2023-05-02 09:03:11
 @RedPacketSec	Node.js @aedart/support module security bypass CVE-2023-30857 - redpacketsecurity.com/node-js-aedart... #CVE #Vulnerability #OSINT #ThreatIntel #Cyber	2023-05-03 09:03:02
 @RedPacketSec	Node.js @aedart/support module security bypass CVE-2023-30857 - redpacketsecurity.com/node-js-aedart... #CVE #Vulnerability #OSINT #ThreatIntel #Cyber	2023-05-04 09:03:29

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2024   |

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](#).

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