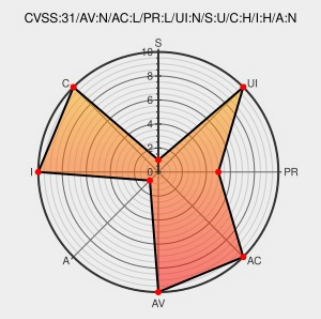
# CVE-2021-29452

Published on: 04/16/2021 12:00:00 AM UTC

Last Modified on: 08/03/2022 10:17:00 AM UTC

## CVE-2021-29452 - advisory for GHSA-8hw9-22v6-9jr9

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




Certain versions of A12n-server from Curveballjs contain the following vulnerability:

a12n-server is an npm package which aims to provide a simple authentication system. A new HAL-Form was added to allow editing users in version 0.18.0. This feature should only have been accessible to admins. Unfortunately, privileges were incorrectly checked allowing any logged in user to make this change. Patched in v0.18.2.

CVE-2021-29452 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **curveball** - **a12n-server** version **>= 0.18 < 0.18.2**

### 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 | NONE | HIGH | NONE |

### CVSS2 Score: 4 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|

| | | |
|---|---|---|
| Any logged in user could edit any other logged in user. · Advisory · curveball/a12n-server · GitHub | github.com text/html | CONFIRM github.com/curveball/a12n-server/security/advisories/GHSA-8hw9-22v6-9jr9 |
| @curveball/a12n-server - npm | www.npmjs.com text/html | MISC www.npmjs.com/package/@curveball/a12n-server |

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.

## Related QID Numbers

982743 Nodejs (npm) Security Update for @curveball/a12n-server (GHSA-8hw9-22v6-9jr9)

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Curveballjs | A12n-server | All | All | All | All |

cpe:2.3:a:curveballjs:a12n-server:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2021-29452 : a12n-server is an npm package which aims to provide a simple authentication system. A new HAL-Form… twitter.com/i/web/status/1… | 2021-04-16 21:37:41 |
| @DarkEagleCyber | CVE-2021-29452 (a12n-server) dlvr.it/RyQfnF | 2021-04-25 21:02:02 |
| @RemotelyAlerts | Severity: ?? \| a12n-server is an npm package which aims... \| CVE-2021-29452 \| Link for more: alerts.remotelyrmm.com/CVE-2021-29452 | 2022-08-03 11:31:09 |
| @LinInfoSec | Npm - CVE-2021-29452: npmjs.com/package/@curve… | 2022-08-03 13:09:35 |
| /r/netcve | CVE-2021-29452 | 2021-04-16 22:05:09 |

← Previous ID  Next ID→