


# Basic-auth app bundle credential exposure in gatsby-source-wordpress

**High** mlgualtieri published GHSA-rqjw-p5vr-c695 on Jul 15, 2021

Package

 **gatsby-source-wordpress** (npm)

Affected versions

<4.0.8; <5.9.2

Patched versions

4.0.8; 5.9.2

Description

Impact

The gatsby-source-wordpress plugin prior to versions 4.0.8 and 5.9.2 leaks .htaccess HTTP Basic Authentication variables into the app.js bundle during build-time. Users who are not initializing basic authentication credentials in the gatsby-config.js are not affected.

Example affected gatsby-config.js:

```
resolve: 'gatsby-source-wordpress',
auth: {
  htaccess: {
    username: leaked_username
    password: leaked_password,
  },
},
```

Patches

A patch has been introduced in gatsby-source-wordpress@4.0.8 and gatsby-source-wordpress@5.9.2 which mitigates the issue by filtering all variables specified in the auth: { } section. Users that depend on this functionality are advised to upgrade to the latest release of gatsby-source-wordpress, run gatsby clean followed by a gatsby build.

Workarounds

There is no known workaround at this time, other than manually editing the app.js file post-build.

For more information

Email us at [security@gatsbyjs.com](mailto:security@gatsbyjs.com)

Severity **High** 7.5 / 10

CVSS base metrics	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None
Availability	None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVE ID  
CVE-2021-32770

Weaknesses  
No CWEs