

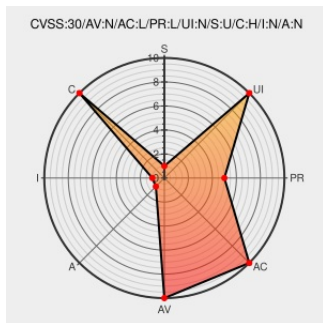


CVE-2018-3712

Published on: 06/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:25 PM UTC

CVE-2018-3712

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

Certain versions of [Serve](#) from [Zeit](#) contain the following vulnerability:
serve node module before 6.4.9 suffers from a Path Traversal vulnerability due to not handling %2e (.) and %2f (/) and allowing them in paths, which allows a malicious user to view the contents of any directory with known path.

CVE-2018-3712 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [h1](#) **HackerOne** - **serve node module** version **Versions before 6.4.9**

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: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
HackerOne	Exploit Technical Description hackerone.com	h1 MISC hackerone.com/reports/307666

hackerone.com
text/html

Scope to working directory correctly by leo · Pull Request #316 · vercel/serve · GitHub

Vendor Advisory
github.com
text/html

MISC
github.com/zeit/serve/pull/316

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

983167 Nodejs (npm) Security Update for serve (GHSA-q2qh-cgc2-qhr3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zeit	Serve	All	All	All	All
Application	Zeit	Serve	All	All	All	All
cpe:2.3:a:zeit:serve:*:*:*:*:*:node.js:*:*						
cpe:2.3:a:zeit:serve:*:*:*:*:*:node.js:*:*						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →