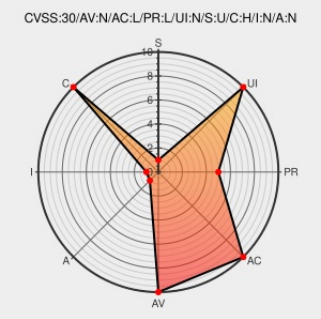
# CVE-2018-3712

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 support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **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<br>Technical Description<br>hackerone.com | MISC<br>hackerone.com/reports/307666 |

| | | |
|---|---|---|
| | text/html | |
| Scope to working directory correctly by leo · Pull Request #316 · vercel/serve · GitHub | Vendor Advisory<br>github.com<br>text/html | MISC<br>github.com/zeit/serve/pull/316 |



## 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→