


File System Bounds Escape

Moderate matt-forster published GHSA-pmw4-jgxx-pcq9 on Dec 16, 2020

Package

 **ftp-srv** (npm)

Affected versions

<= 4.3.4

Patched versions

None

Description

Impact

Clients of FTP servers utilizing `ftp-srv` hosted on Windows machines can escape the FTP user's defined root folder using the expected FTP commands, for example, `CWD` and `UPDR`.

Background

When windows separators exist within the path (`\`), `path.resolve` leaves the upper pointers intact and allows the user to move beyond the root folder defined for that user. We did not take that into account when creating the path resolve function.

```
const path = require('path'); *1

path.resolve('..../..') //= '/' *1
path.resolve('..\..\..\') //= '/..\..\..' *1
```

Patches

None at the moment.

Workarounds

There are no workarounds for windows servers. Hosting the server on a different OS mitigates the issue.

References

Issues:
[#167](#)
[#225](#)

For more information

If you have any questions or comments about this advisory:
Open an issue at <https://github.com/autovance/ftp-srv>.
Please email us directly; security@autovance.com.

Severity

Moderate

CVE ID

CVE-2020-26299

Weaknesses

No CWEs

Credits

 n-timofeev