Exposure of home directory through shescape on Unix with Bash

Low ericcornelissen published GHSA-446w-rrm4-r47f on Mar 3

Package

shescape (npm)

Affected versions

>=1.4.0 <1.5.1

Patched versions

1.5.1

Description

Impact

The issue allows for exposure of the home directory on Unix systems when using Bash with the `escape` or `escapeAll` functions from the *shescape* API with the `interpolation` option set to `true`. Other tested shells, Dash and Zsh, are not affected.

```
const cp = require("child_process");
const shescape = require("shescape");

const payload = "home_directory=~";
const options = { interpolation: true };
console.log(cp.execSync(`echo ${shescape.escape(payload, options)}`));
// home_directory=/home/user
```

Depending on how the output of *shescape* is used, directory traversal may be possible in the application using *shescape*.

Patches

The issue was patched in `v1.5.1`.

Workarounds

Manually escape all instances of the tilde character (`~`) using `arg.replace(/~/g, "\\~")`.

References

See GitHub issue #169.

Severity

Low

CVE ID

CVE-2022-24725

Weaknesses

CWE-200