

Insufficient escaping of line feeds for CMD

Moderate ericcornelissen published GHSA-jjc5-fp7p-6f8w on Jul 15

Package

 **shescape** (npm)

Affected versions

<1.5.8

Patched versions

1.5.8

Description

Impact

This impacts users that use Shescape (any API function) to escape arguments for **cmd.exe** on **Windows**. An attacker can omit all arguments following their input by including a line feed character (`'\n'`) in the payload. Example:


```
import cp from "node:child_process";
import * as shescape from "shescape";

// 1. Prerequisites
const options = {
  shell: "cmd.exe",
};

// 2. Attack
const payload = "attacker\n";

// 3. Usage
let escapedPayload;
escapedPayload = shescape.escape(payload, options);
// Or
escapedPayload = shescape.escapeAll([payload], options)[0];
// Or
escapedPayload = shescape.quote(payload, options);
// Or
escapedPayload = shescape.quoteAll([payload], options)[0];
```

```
cp.execSync(`echo Hello ${escapedPayload}! How are you doing?`, options);  
// Outputs: "Hello attacker"
```

 **Note:** `execSync` is just illustrative here, all of `exec`, `execFile`, `execFileSync`, `fork`, `spawn`, and `spawnSync` can be attacked using a line feed character if CMD is the shell being used.

Patches

This bug has been patched in [v1.5.8](#) which you can upgrade to now. No further changes are required.

Workarounds

Alternatively, line feed characters (`'\n'`) can be stripped out manually or the user input can be made the last argument (this only limits the impact).

References

- [#332](#)
- <https://github.com/ericcornelissen/shescape/releases/tag/v1.5.8>

For more information

If you have any questions or comments about this advisory:

- Comment on [#332](#)
- Open an issue at <https://github.com/ericcornelissen/shescape/issues> (*New issue > Question > Get started*)

Severity

Moderate

CVE ID

CVE-2022-31179

Weaknesses

CWE-150