Insufficient escaping of whitespace

High ericcornelissen published GHSA-44vr-rwwj-p88h on Jul 15

Package

shescape (npm)

Affected versions

>=1.4.0 < 1.5.8

Patched versions

1.5.8

Description

Impact

This only impacts users that use the `escape` or `escapeAll` functions with the `interpolation` option set to `true`. Example:

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

// 1. Prerequisites
const options = {
  shell: "bash",
  // Or
  shell: "dash",
  // Or
  shell: "powershell.exe",
  // Or
  shell: "zsh",
  // Or
  shell: undefined, // Only if the default shell is one of the affected shells.
};

// 2. Attack (one of multiple)
const payload = "foo #bar";

// 3. Usage
let escapedPayload;
shescape.escape(payload, { interpolation: true });
// Or
shescape.escapeAll(payload, { interpolation: true });
```

```
cp.execSync(`echo Hello ${escapedPayload}!`, options);
// _Output depends on the shell being used_
```

The result is that if an attacker is able to include whitespace in their input they can:

1. Invoke shell-specific behaviour through shell-specific special characters inserted directly after whitespace.
   - Affected shells: *Bash*, *Dash*, *Zsh*, *PowerShell*
2. Invoke shell-specific behaviour through shell-specific special characters inserted or appearing after line terminating characters.
   - Affected shells: *Bash*
3. Invoke arbitrary commands by inserting a line feed character.
   - Affected Shells: *Bash*, *Dash*, *Zsh*, *PowerShell*
4. Invoke arbitrary commands by inserting a carriage return character.
   - Affected Shells: *PowerShell*

Patches

Behaviour number 1 has been patched in v1.5.7 which you can upgrade to now. No further changes are required.

Behaviour number 2, 3, and 4 have been patched in v1.5.8 which you can upgrade to now. No further changes are required.

Workarounds

The best workaround is to avoid having to use the `interpolation: true` option - in most cases using an alternative is possible, see the recipes for recommendations.

Alternatively, you can strip all whitespace from user input. Note that this is error prone, for example: for PowerShell this requires stripping `'\u0085'` which is not included in JavaScript's definition of `\s` for Regular Expressions.

References

- #322
- #324
- #332
- https://github.com/ericcornelissen/shescape/releases/tag/v1.5.7
- https://github.com/ericcornelissen/shescape/releases/tag/v1.5.8

For more information

- Comment on:
  - For behaviour 1 (PowerShell): #322

    - For behaviour 1 (Bash, Dash, Zsh): #324
    - For behaviour 2, 3, 4 (*any shell*): #332
- Open an issue at https://github.com/ericcornelissen/shescape/issues (*New issue* > *Question* > *Get started*)
- If you're missing CMD from this advisory, see GHSA-jjc5-fp7p-6f8w

Severity

High

CVE ID

CVE-2022-31180

Weaknesses

CWE-150 CWE-200