Null characters not escaped

High ericcornelissen published GHSA-f2rp-38vg-j3gh on Mar 13, 2021

Package

shescape (npm)

Affected versions	Patched versions
< 1.1.3	1.1.3

Description

Impact

Anyone using *Shescape* to defend against shell injection may still be vulnerable against shell injection if the attacker manages to insert a null character into the payload. For example (on Windows):

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

const nullChar = String.fromCharCode(0);
const payload = "foo\" && ls -al ${nullChar} && echo \"bar";
console.log(cp.execSync(`echo ${shescape.quote(payload)}`));
// foototal 3
// drwxr-xr-x 1 owner XXXXXX      0 Mar 13 18:44 .
// drwxr-xr-x 1 owner XXXXXX      0 Mar 13 00:09 ..
// drwxr-xr-x 1 owner XXXXXX      0 Mar 13 18:42 folder
// -rw-r--r-- 1 owner XXXXXX      0 Mar 13 18:42 file
```

Patches

The problem has been patched in v1.1.3 which you can upgrade to now. No further changes are required.

Workarounds

Alternatively, null characters can be stripped out manually using e.g. `arg.replace(/\u{0}/gu, "")`

Severity

High

CVE ID

CVE-2021-21384

Weaknesses

No CWEs