New issue

Jump to bottom

Security bug in hue-magic.js #217

Closed **martinzhou2015** opened this issue on Jan 17, 2021 · 1 comment

Labels bug

martinzhou2015 commented on Jan 17, 2021 • edited

Describe the bug

The `res.sendFile` API, used in file `hue-magic.js`, introduces a `Path Traversal` vulnerability.

node-red-contrib-huemagic/huemagic/hue-magic.js
Line 277 in 4cb9d2e

```
277     res.sendFile(path.resolve(__dirname, 'animations', 'previews', req.params.file));
```

Flow to Reproduce
Since the path isn't protected by `RED.auth.needsPermission` API, the attacker could fetch arbitrary file on the server with the PoC below directly.

```
http://target_host/hue/assets/..%2F..%2F..%2F..%2F..%2F..%2Fetc%2fpasswd
```

Expected behavior
To fix this vulnerability, `option` of the `res.sendFile` should be specified correctly.

```
res.sendFile(path [, options] [, fn])

dotfiles : deny
```

martinzhou2015 added the bug label on Jan 17, 2021

Foddy added a commit that referenced this issue on Jan 9

Update to v4.0.0 ··· 7d45a64

Foddy commented on Jan 9 Owner

Thank you very much. This has been fixed in the newest update. Better late than never :S

Foddy closed this as completed on Jan 9

Akokonunes mentioned this issue on Jan 29

Create CVE-2021-25864.yaml projectdiscovery/nuclei-templates#3631

Merged

Assignees
No one assigned

Labels
bug

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants