Path Traversal in socket.io-file

High severity GitHub Reviewed Published on Jul 7, 2020 • Updated on Sep 22, 2021

Vulnerability details Dependabot alerts 0

Package

socket.io-file (npm)

Affected versions	Patched versions
<= 2.0.31	None

Description

All versions of `socket.io-file` are vulnerable to Path Traversal. The package fails to sanitize user input and uses it to generate the file upload paths. The `socket.io-file::createFile` message contains a `name` option that is passed directly to `path.join()` . It is possible to upload files to arbitrary folders on the server by sending relative paths on the `name` value, such as `../../test.js` . The `uploadDir` and `rename` options can be used to define the file upload path.

References

- https://www.npmjs.com/advisories/1519
- https://nvd.nist.gov/vuln/detail/CVE-2020-15779
- GHSA-9h4g-27m8-qjrg
- https://github.com/rico345100/socket.io-file
- https://www.npmjs.com/package/socket.io-file

Severity

High 7.5 / 10

CVSS base metrics	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Weaknesses

CWE-22

CVE ID

CVE-2020-15779

GHSA ID

GHSA-9h4g-27m8-qjrg

Source code

rico345100/socket.io-file

This advisory has been edited. See History.

See something to contribute? Suggest improvements for this vulnerability.