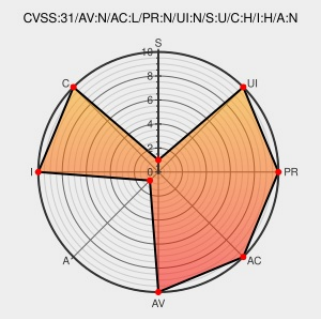
CVE-2022-31183

Published on: Not Yet Published

Last Modified on: 08/09/2022 07:38:00 PM UTC

CVE-2022-31183 - advisory for GHSA-2cpx-6pqp-wf35

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fs2 from Typelevel contain the following vulnerability:

fs2 is a compositional, streaming I/O library for Scala. When establishing a server-mode `TLSSocket` using `fs2-io` on Node.js, the parameter `requestCert = true` is ignored, peer certificate verification is skipped, and the connection proceeds. The vulnerability is limited to: 1. `fs2-io` running on Node.js. The JVM TLS implementation is completely independent. 2. `TLSSocket`s in server-mode. Client-mode `TLSSocket`s are implemented via a different API. 3. mTLS as enabled via `requestCert = true` in `TLSParameters`. The default setting is `false` for server-mode `TLSSocket`s. It was introduced with the initial Node.js implementation of fs2-io in 3.1.0. A patch is released in v3.2.11. The requestCert = true parameter is respected and the peer certificate is verified. If verification fails, a SSLException is raised. If using an unpatched version on Node.js, do not use a server-mode TLSSocket with requestCert = true to establish a mTLS connection.

CVE-2022-31183 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **typelevel** - **fs2** version **>= 3.1.0, < 3.2.11**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
mTLS client verification is skipped in	github.com	CONFIRM github.com/typelevel/fs2/security/advisories/GHSA-2cpx-6pqp-

Node.js TLS server · Advisory · typelevel/fs2 · GitHub	text/html	wf35
How to use `new tls.TLSSocket(...)` to establish a secure connection? · Issue #43994 · nodejs/node · GitHub	github.com text/html	MISC github.com/nodejs/node/issues/43994
First attempt at test for GHSA-2cpx-6pqp-wf35 · typelevel/fs2@6598243 · GitHub	github.com text/html	MISC github.com/typelevel/fs2/commit/659824395826a314e0a4331535dbf1ef8bef8207

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typelevel	Fs2	All	All	All	All

cpe:2.3:a:typelevel:fs2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31183 : fs2 is a compositional, streaming I/O library for Scala. When establishing a server-mode `TLSSocke… twitter.com/i/web/status/1…	2022-08-01 19:56:15
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-31183 fs2 is a compositional, streaming I/O library for Scala. When est… twitter.com/i/web/status/1…	2022-08-01 21:56:00
@LinInfoSec	Nodejs - CVE-2022-31183: github.com/typelevel/fs2/…	2022-08-01 23:01:41
/r/netcve	CVE-2022-31183	2022-08-01 20:38:20

← Previous ID

Next ID→