

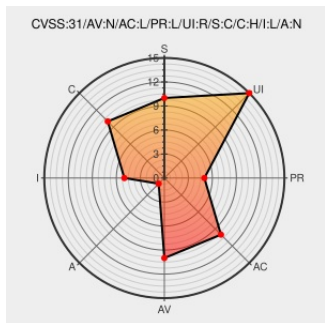


CVE-2020-5280

Published on: 03/25/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:04 PM UTC

CVE-2020-5280 - advisory for GHSA-66q9-f7ff-mmx6

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Http4s](#) from [Typelevel](#) contain the following vulnerability:

http4s before versions 0.18.26, 0.20.20, and 0.21.2 has a local file inclusion vulnerability. This vulnerability applies to all users of `org.http4s.server.staticcontent.FileService`, `org.http4s.server.staticcontent.ResourceService` and `org.http4s.server.staticcontent.WebjarService`. URI normalization is

applied incorrectly. Requests whose path info contain `../` or `//` can expose resources outside of the configured location. This issue is patched in versions 0.18.26, 0.20.20, and 0.21.2. Note that 0.19.0 is a deprecated release and has never been supported.

CVE-2020-5280 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [http4s](#) - **http4s** version < 0.18.26

Affected Vendor/Software: [http4s](#) - **http4s** version >= 0.19.0, < 0.20.20

Affected Vendor/Software: [http4s](#) - **http4s** version >= 0.21.0, < 0.21.2

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

impact

PARTIAL

impact

NONE

impact

NONE

CVE References

Description	Tags	Link
Merge pull request from GHSA-66q9-f7ff-mmx6 · http4s/http4s@b87f31b · GitHub	Patchgithub.comtext/html	MISCgithub.com/http4s/http4s/commit/b87f31b2292dabe667bec3b04ce66176c8a3e17b
Local file inclusion vulnerability in FileService, ResourceService, WebjarService · Advisory · http4s/http4s · GitHub	Third Party Advisorygithub.comtext/html	CONFIRMgithub.com/http4s/http4s/security/advisories/GHSA-66q9-f7ff-mmx6
Merge pull request from GHSA-66q9-f7ff-mmx6 · http4s/http4s@250afdd · GitHub	Patchgithub.comtext/html	MISCgithub.com/http4s/http4s/commit/250afddb2e65b70ca9ddaec9d1eb3aaa56de7ec
Merge pull request from GHSA-66q9-f7ff-mmx6 · http4s/http4s@752b3f6 · GitHub	Patchgithub.comtext/html	MISCgithub.com/http4s/http4s/commit/752b3f63a05a31d2de4f8706877aa08d6b89efca

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.

Related QID Numbers

982989 Java (maven) Security Update for org.http4s:http4s-server_2.12 (GHSA-66q9-f7ff-mmx6)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typelevel	Http4s	All	All	All	All
Application	Typelevel	Http4s	All	All	All	All

cpe:2.3:a:typelevel:http4s:*****::

cpe:2.3:a:typelevel:http4s:*****::

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report