



CVE-2021-32643

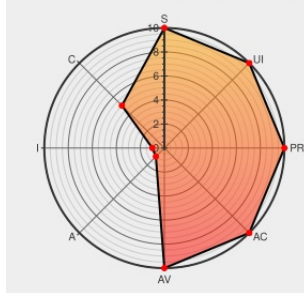
Published on: 05/27/2021 12:00:00 AM UTC

Last Modified on: 06/10/2021 01:32:00 PM UTC

CVE-2021-32643 - advisory for GHSA-6h7w-fc84-x7p6

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N



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

Http4s is a Scala interface for HTTP services. `StaticFile.fromUri` can leak the presence of a directory on a server when the `URL` scheme is not `file://`, and the URL points to a fetchable resource under its scheme and authority. The function returns `F[None]`, indicating no resource, if `url.getFile` is a directory, without first checking the scheme

or authority of the URL. If a URL connection to the scheme and URL would return a stream, and the path in the URL exists as a directory on the server, the presence of the directory on the server could be inferred from the 404 response. The contents and other metadata about the directory are not exposed. This affects http4s versions: 0.21.7 through 0.21.23, 0.22.0-M1 through 0.22.0-M8, 0.23.0-M1, and 1.0.0-M1 through 1.0.0-M22. The [patch] (<https://github.com/http4s/http4s/commit/52e1890665410b4385e37b96bc49c5e3c708e4e9>) is available in the following versions: v0.21.24, v0.22.0-M9, v0.23.0-M2, v1.0.0-M23. As a workaround users can avoid calling `StaticFile.fromUri` with non-file URLs.

CVE-2021-32643 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [http4s](#) - [http4s](#) version $\geq 0.21.7$, $< 0.21.24$

Affected Vendor/Software: [http4s](#) - [http4s](#) version $\geq 0.22.0-M1$, $\leq 0.22.0-M8$

Affected Vendor/Software: [http4s](#) - [http4s](#) version $= 0.23.0-M1$

Affected Vendor/Software: [http4s](#) - [http4s](#) version $\geq 1.0.0-M1$, $< 1.0.0-M23$

CVSS3 Score: **5.8 - MEDIUM**

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

CHANGED	LOW	NONE	NONE
CVSS2 Score: 5 - MEDIUM			
Access Vector	Access Complexity	Authentication	
NETWORK	LOW	NONE	
Confidentiality Impact	Integrity Impact	Availability Impact	
PARTIAL	NONE	NONE	

CVE References

Description	Tags	Link
Fix directory leak in StaticFile.fromUrl · http4s/http4s@52e1890 · GitHub	github.com text/html	MISC github.com/http4s/http4s/commit/52e1890665410b4385e37b96bc49c5e3c708e4e9
StaticFile.fromUrl can leak presence of a directory · Advisory · http4s/http4s · GitHub	github.com text/html	CONFIRM github.com/http4s/http4s/security/advisories/GHSA-6h7w-fc84-x7p6
Maven Repository: org.http4s » http4s-core	web.archive.org text/html Inactive Link Not Archived	MISC mvnrepository.com/artifact/org.http4s/http4s-core

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

983827 Java (maven) Security Update for org.http4s:http4s-core (GHSA-6h7w-fc84-x7p6)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typelevel	Http4s	All	All	All	All
Application	Typelevel	Http4s	0.22.0	milestone1	All	All
Application	Typelevel	Http4s	0.22.0	milestone2	All	All
Application	Typelevel	Http4s	0.22.0	milestone3	All	All
Application	Typelevel	Http4s	0.22.0	milestone4	All	All
Application	Typelevel	Http4s	0.22.0	milestone5	All	All
Application	Typelevel	Http4s	0.22.0	milestone6	All	All
Application	Typelevel	Http4s	0.22.0	milestone7	All	All
Application	Typelevel	Http4s	0.22.0	milestone8	All	All

Application	Typelevel	Http4s	0.23.0	milestone1	All	All
Application	Typelevel	Http4s	1.0.0	milestone1	All	All
Application	Typelevel	Http4s	1.0.0	milestone10	All	All
Application	Typelevel	Http4s	1.0.0	milestone11	All	All
Application	Typelevel	Http4s	1.0.0	milestone12	All	All
Application	Typelevel	Http4s	1.0.0	milestone13	All	All
Application	Typelevel	Http4s	1.0.0	milestone14	All	All
Application	Typelevel	Http4s	1.0.0	milestone15	All	All
Application	Typelevel	Http4s	1.0.0	milestone16	All	All
Application	Typelevel	Http4s	1.0.0	milestone17	All	All
Application	Typelevel	Http4s	1.0.0	milestone18	All	All
Application	Typelevel	Http4s	1.0.0	milestone19	All	All
Application	Typelevel	Http4s	1.0.0	milestone2	All	All
Application	Typelevel	Http4s	1.0.0	milestone20	All	All
Application	Typelevel	Http4s	1.0.0	milestone21	All	All
Application	Typelevel	Http4s	1.0.0	milestone22	All	All
Application	Typelevel	Http4s	1.0.0	milestone3	All	All
Application	Typelevel	Http4s	1.0.0	milestone4	All	All
Application	Typelevel	Http4s	1.0.0	milestone5	All	All
Application	Typelevel	Http4s	1.0.0	milestone6	All	All
Application	Typelevel	Http4s	1.0.0	milestone7	All	All
Application	Typelevel	Http4s	1.0.0	milestone8	All	All
Application	Typelevel	Http4s	1.0.0	milestone9	All	All
cpe:2.3:a:typelevel:http4s:*:*:*:*:*:						
cpe:2.3:a:typelevel:http4s:0.22.0:milestone1:*:*:*:*:						
cpe:2.3:a:typelevel:http4s:0.22.0:milestone2:*:*:*:*:						
cpe:2.3:a:typelevel:http4s:0.22.0:milestone3:*:*:*:*:						
cpe:2.3:a:typelevel:http4s:0.22.0:milestone4:*:*:*:*:						
cpe:2.3:a:typelevel:http4s:0.22.0:milestone5:*:*:*:*:						
cpe:2.3:a:typelevel:http4s:0.22.0:milestone6:*:*:*:*:						
cpe:2.3:a:typelevel:http4s:0.22.0:milestone7:*:*:*:*:						
cpe:2.3:a:typelevel:http4s:0.22.0:milestone8:*:*:*:*:						
cpe:2.3:a:typelevel:http4s:0.23.0:milestone1:*:*:*:*:						

cpe:2.3:a:ypelevel:http4s:1.0.0:milestone1:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone10:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone11:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone12:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone13:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone14:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone15:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone16:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone17:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone18:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone19:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone2:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone20:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone21:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone22:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone3:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone4:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone5:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone6:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone7:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone8:*****:
cpe:2.3:a:ypelevel:http4s:1.0.0:milestone9:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-32643 : Http4s is a Scala interface for HTTP services. `StaticFile.fromUri` can leak the presence of a dir... twitter.com/i/web/status/1...	2021-05-27 17:16:44
 /r/netcve	CVE-2021-32643	2021-05-27 17:41:49

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)