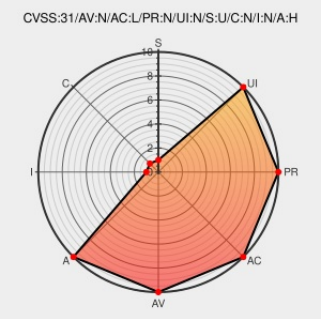
CVE-2022-24668

Published on: 02/09/2022 12:00:00 AM UTC

Last Modified on: 02/22/2022 06:53:00 PM UTC

CVE-2022-24668

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



Certain versions of Swiftnio Http/2 from Apple contain the following vulnerability:

A program using swift-nio-http2 is vulnerable to a denial of service attack caused by a network peer sending ALTSVC or ORIGIN frames. This attack affects all swift-nio-http2 versions from 1.0.0 to 1.19.1. This vulnerability is caused by a logical error after frame parsing but before frame handling. ORIGIN and ALTSVC frames are not currently supported by swift-nio-http2, and should be ignored. However, one code path that encounters them has a deliberate trap instead. This was left behind from the original development process and was never removed. Sending an ALTSVC or ORIGIN frame does not require any special permission, so any HTTP/2 connection peer may send such a frame. For clients, this means any server to which they connect may launch this attack. For servers, anyone they allow to connect to them may launch such an attack. The attack is low-effort: it takes very little resources to send one of these frames. The impact on availability is high: receiving the frame immediately crashes the server, dropping all in-flight connections and causing the service to need to restart. It is straightforward for an attacker to repeatedly send these frames, so attackers require very few resources to achieve a substantial denial of service. The attack does not have any confidentiality or integrity risks in and of itself. This is a controlled, intentional crash. However, sudden process crashes can lead to violations of invariants in services, so it is possible that this attack can be used to trigger an error condition that has confidentiality or integrity risks. The risk can be mitigated if untrusted peers can be prevented from communicating with the service. This mitigation is not available to many services. The issue is fixed by rewriting the parsing code to correctly handle the condition. The issue was found by automated fuzzing by oss-fuzz.

CVE-2022-24668 has been assigned by cve@forums.swift.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Swift Project** - **SwiftNIO HTTP2** version **>= 1.0.0**

Affected Vendor/Software: **Swift Project** - **SwiftNIO HTTP2** version **<= 1.19.1**

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	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
	github.com text/plain Inactive Link Not Archived	MISC github.com/apple/swift-nio-http2/security/advisories/GHSA-pgfx-g6rc-8cjv

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	Apple	Swiftnio Http/2	All	All	All	All

cpe:2.3:a:apple:swiftnio_http\/2:*:*:*:*:*:swift:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-24668 : A program using swift-nio-http2 is vulnerable to a denial of service attack caused by a network pe… twitter.com/i/web/status/1…	2022-02-09 23:36:18
@SecRiskRptSME	RT: CVE-2022-24668 A program using swift-nio-http2 is vulnerable to a denial of service attack caused by a network… twitter.com/i/web/status/1…	2022-02-10 08:33:40
/r/netcve	CVE-2022-24668	2022-02-10 00:39:03

← Previous ID

Next ID→

© 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 registred 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