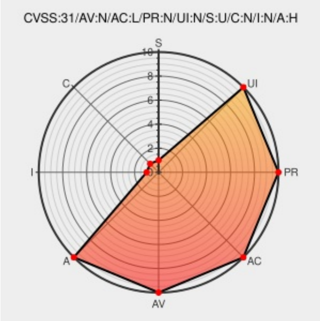
CVE-2022-3252

Published on: Not Yet Published

Last Modified on: 09/26/2022 10:11:00 PM UTC

CVE-2022-3252

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



Certain versions of Swift-nio-extras from Apple contain the following vulnerability:

Improper detection of complete HTTP body decompression SwiftNIO Extras provides a pair of helpers for transparently decompressing received HTTP request or response bodies. These two objects (HTTPRequestDecompressor and HTTPResponseDecompressor) both failed to detect when the decompressed body was considered complete. If trailing junk data was appended to the HTTP message body, the code would repeatedly attempt to decompress this data and fail. This would lead to an infinite loop making no forward progress, leading to livelock of the system and denial-of-service. This issue can be triggered by any attacker capable of sending a compressed HTTP message. Most commonly this is HTTP servers, as compressed HTTP messages cannot be negotiated for HTTP requests, but it is possible that users have configured decompression for HTTP requests as well. The attack is low effort, and likely to be reached without requiring any privilege or system access. The impact on availability is high: the process immediately becomes unavailable but does not immediately crash, meaning that it is possible for the process to remain in this state until an administrator intervenes or an automated circuit breaker fires. If left unchecked this issue will very slowly exhaust memory resources due to repeated buffer allocation, but the buffers are not written to and so it is possible that the processes will not terminate for quite some time. This risk can be mitigated by removing transparent HTTP message decompression. The issue is fixed by correctly detecting the termination of the compressed body as reported by zlib and refusing to decompress further data. The issue was found by Vojtech Rylko (https://github.com/vojtarylko) and reported publicly on GitHub.

CVE-2022-3252 has been assigned by cve@forums.swift.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Swift Project** - **SwiftNIO Extras** version < **1.14.0**

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

CVE References

Description	Tags	Link
Improper detection of complete HTTP body decompression · Advisory · apple/swift-nio-extras · GitHub	github.com text/html	MISC github.com/apple/swift-nio-extras/security/advisories/GHSA-773g-x274-8qmf

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	Swift-nio-extras	All	All	All	All

cpe:2.3:a:apple:swift-nio-extras:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-3252 : Improper detection of complete HTTP body decompression SwiftNIO Extras provides a pair of helpers f… twitter.com/i/web/status/1…	2022-09-21 19:05:47
/r/netcve	CVE-2022-3252	2022-09-21 20:38:43

← Previous ID

Next ID→

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