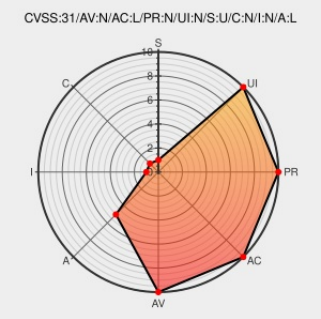
CVE-2022-29189

Published on: Not Yet Published

Last Modified on: 06/03/2022 01:59:00 AM UTC

CVE-2022-29189 - advisory for GHSA-cx94-mrg9-rq4j

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



Certain versions of Dtls from Pion contain the following vulnerability:

Pion DTLS is a Go implementation of Datagram Transport Layer Security. Prior to version 2.1.4, a buffer that was used for inbound network traffic had no upper limit. Pion DTLS would buffer all network traffic from the remote user until the handshake completes or timed out. An attacker could exploit this to cause excessive memory usage. Version 2.1.4 contains a patch for this issue. There are currently no known workarounds available.

CVE-2022-29189 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **pion** - **dtls** version **< 2.1.4**

CVSS3 Score: 5.3 - MEDIUM

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

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

Description	Tags	Link
Add limit to fragmentBuffer · pion/dtls@a6397ff · GitHub	github.com text/html	MISC github.com/pion/dtls/commit/a6397ff7282bc56dc37a68ea9211702edb4de1de
Buffer for inbound DTLS fragments has no limit · Advisory · pion/dtls · GitHub	github.com text/html	CONFIRM github.com/pion/dtls/security/advisories/GHSA-cx94-mrg9-rq4j
Release v2.1.4 · pion/dtls · GitHub	github.com text/html	MISC github.com/pion/dtls/releases/tag/v2.1.4

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

184297 Debian Security Update for snowflake (CVE-2022-29189)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pion	Dtls	All	All	All	All

cpe:2.3:a:pion:dtls:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29189 : Pion DTLS is a Go implementation of Datagram Transport Layer Security. Prior to version 2.1.4, a b… twitter.com/i/web/status/1…	2022-05-21 00:03:50
/r/netcve	CVE-2022-29189	2022-05-21 01:38:54

← Previous ID

Next ID→