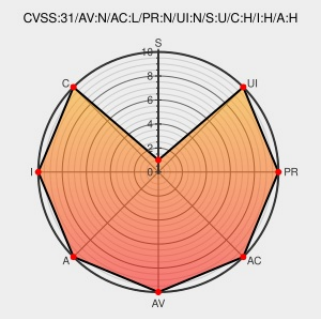
CVE-2019-20786

Published on: 04/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:50 PM UTC

CVE-2019-20786

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



Certain versions of Dtls from Pion contain the following vulnerability:

handleIncomingPacket in conn.go in Pion DTLS before 1.5.2 lacks a check for application data with epoch 0, which allows remote attackers to inject arbitrary unencrypted data after handshake completion.

CVE-2019-20786 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Analysis of DTLS Implementations Using Protocol State Fuzzing | USENIX	Third Party Advisory, www.usenix.org, text/html	MISC www.usenix.org/conference/usenixsecurity20/presentation/fiterau-brostean
	Exploit	MISC www.usenix.org/system/files/sec20fall_fiterau-

	Third Party Advisory www.usenix.org application/pdf	brostean_prepub.pdf
Comparing v1.5.1...v1.5.2 · pion/dtls · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/pion/dtls/compare/v1.5.1...v1.5.2
Assert that ApplicationData has epoch != 0 · pion/dtls@fd73a5d · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/pion/dtls/commit/fd73a5df2ff0e1fb6ae6a51e2777d7a16cc4f4e0

Related QID Numbers

982031 Go (go) Security Update for github.com/pion/dtls (GHSA-7gfg-6934-mqq2)

Known Affected Configurations (CPE V2.3)

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→