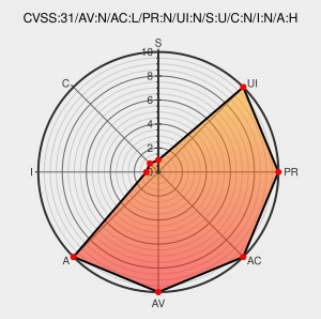
CVE-2019-11937

Published on: 12/04/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:36 PM UTC

CVE-2019-11937

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



Certain versions of Mcrouter from Facebook contain the following vulnerability:

In Mcrouter prior to v0.41.0, a large struct input provided to the Carbon protocol reader could result in stack exhaustion and denial of service.

CVE-2019-11937 has been assigned by cve-assign@fb.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Facebook** - **Mcrouter** version **!=> 0.41.0**

Affected Vendor/Software: **Facebook** - **Mcrouter** version **< 0.41.0**

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

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

Facebook	Vendor Advisory www.facebook.com text/html	CONFIRM www.facebook.com/security/advisories/cve-2019-11937
Attempt to make CarbonProtocolReader::skip tail recursive · facebook/mcrouter@97e033b · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/facebook/mcrouter/commit/97e033b3bb0cb16b61bf49f0dc7f311a3e0edd1b
Release Version 41 · facebook/mcrouter · GitHub	Release Notes Vendor Advisory github.com text/html	MISC github.com/facebook/mcrouter/releases/tag/v0.41.0-release

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Facebook	Mcrouter	All	All	All	All
Application	Facebook	Mcrouter	All	All	All	All

cpe:2.3:a:facebook:mcrouter:*:*:*:*:*:*:*:*:

cpe:2.3:a:facebook:mcrouter:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→