



CVE-2019-11938

Published on: 03/10/2020 12:00:00 AM UTC

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

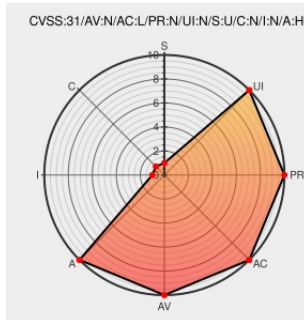
CVE-2019-11938

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Thrift](#) from [Facebook](#) contain the following vulnerability:

Java Facebook Thrift servers would not error upon receiving messages declaring containers of sizes larger than the payload. As a result, malicious clients could send short messages which would result in a large memory allocation, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2019.12.09.00.

CVE-2019-11938 has been assigned by [cve-assign@fb.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Facebook](#) - Facebook Thrift version $\geq$ v2019.12.09.00

Affected Vendor/Software: [Facebook](#) - Facebook Thrift version $<$ v2019.12.09.00

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-2019-11938

Java: Check the size of the remaining frame before deserializing a st... · facebook/fbthrift@08c2d41 · GitHub

Patch
Third Party Advisory
github.com
text/html

MISC
github.com/facebook/fbthrift/commit/08c2d412adb214c40bb03be7587057b25d053030

Java: Check the size of the remaining frame before deserializing coll... · facebook/fbthrift@71c97ff · GitHub

Patch
Third Party Advisory
github.com
text/html

MISC
github.com/facebook/fbthrift/commit/71c97ffdc61cccf1f8267774e873e21ebd3ebd3

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	Facebook	Thrift	All	All	All	All
Application	Facebook	Thrift	All	All	All	All

cpe:2.3:a:facebook:thrift:*****:

cpe:2.3:a:facebook:thrift:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →