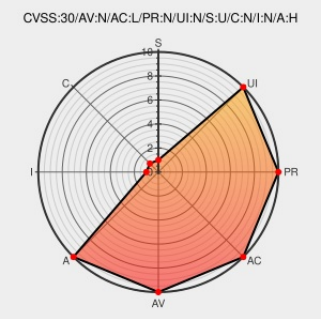
CVE-2018-6347

Published on: 12/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:47 PM UTC

CVE-2018-6347

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



Certain versions of Proxygen from Proxygen Project contain the following vulnerability:

An issue in the Proxygen handling of HTTP2 parsing of headers/trailers can lead to a denial-of-service attack. This affects Proxygen prior to v2018.12.31.00.

CVE-2018-6347 has been assigned by cve-assign@fb.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Facebook** - **Proxygen** version **!=> v2018.12.31.00**

Affected Vendor/Software: **Facebook** - **Proxygen** version **<= v2018.12.31.00**

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

Don't lower lastStreamID_ · facebook/proxygen@223e0aa · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/facebook/proxygen/commit/223e0aa6bc7590e86af1e917185a2e0efe16071

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Proxygen Project	Proxygen	All	All	All	All
Application	Proxygen Project	Proxygen	All	All	All	All

cpe:2.3:a:proxygen_project:proxygen:*:*:*:*:*:*:*:*:

cpe:2.3:a:proxygen_project:proxygen:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→