

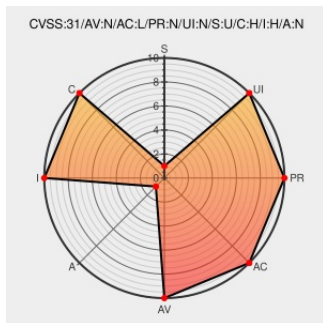


CVE-2020-1887

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

Last Modified on: 03/23/2021 11:23:46 PM UTC

CVE-2020-1887

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Osquery](#) from [Linuxfoundation](#) contain the following vulnerability:

Incorrect validation of the TLS SNI hostname in osquery versions after 2.9.0 and before 4.2.0 could allow an attacker to MITM osquery traffic in the absence of a configured root chain of trust.

CVE-2020-1887 has been assigned by [cve-assign@fb.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Facebook](#) - **Osquery** version **!=> 4.2.0**

Affected Vendor/Software: [Facebook](#) - **Osquery** version **> 2.9.0**

Affected Vendor/Software: [Facebook](#) - **Osquery** version **!=< 2.9.0**

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description

Facebook

Third Party Advisory
www.facebook.com
text/html

CONFIRM
www.facebook.com/security/advisories/cve-2020-1887

http_client: Improve certificate verification by alessandroاريو · Pull Request #6197 · osquery/osquery · GitHub

Patch
Third Party Advisory
github.com
text/html

CONFIRM
github.com/osquery/osquery/pull/6197

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	Linuxfoundation	Osquery	All	All	All	All
Application	Linuxfoundation	Osquery	All	All	All	All

cpe:2.3:a:linuxfoundation:osquery:*****:

cpe:2.3:a:linuxfoundation:osquery:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →