

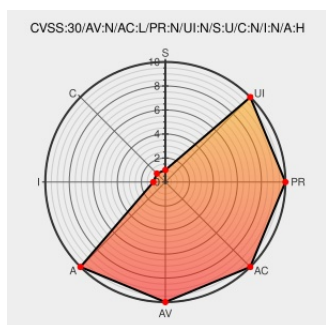


CVE-2019-15541

Published on: 08/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-15541

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

Certain versions of [Rustls](#) from [Rustls Project](#) contain the following vulnerability:

rustls-mio/examples/tlsserver.rs in the rustls crate before 0.16.0 for Rust allows attackers to cause a denial of service (loop of conn_event and ready) by arranging for a client to never be writable.

CVE-2019-15541 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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
tlsserver: fix loop when client will never be writable · ctz/rustls@a93ee1a · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ctz/rustls/commit/a93ee1abd2ab19ebe4bf9d684d56637ee54a6074

Comparing cd66549...17ee52c · ctz/rustls · GitHub

Release Notes

Third Party Advisory

github.com

text/html

MISC

github.com/ctz/rustls/compare/cd66549...17ee52c

bug in rustls-mio · Issue #285 · ctz/rustls · GitHub

Exploit

Issue Tracking

Third Party Advisory

github.com

text/html

MISC

github.com/ctz/rustls/issues/285

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	Rustls Project	Rustls	All	All	All	All
Application	Rustls Project	Rustls	All	All	All	All

cpe:2.3:a:rustls_project:rustls:~::~::~::~::

cpe:2.3:a:rustls_project:rustls:~::~::~::~::

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →