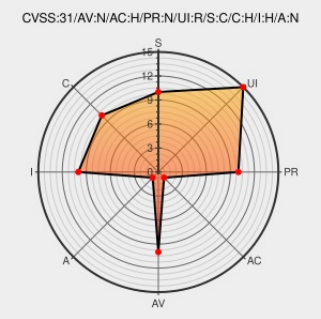
CVE-2020-15133

Published on: 07/31/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 06:28:00 PM UTC

CVE-2020-15133 - advisory for GHSA-2v5c-755p-p4gv

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



Certain versions of Faye-websocket from Faye-websocket Project contain the following vulnerability:

In faye-websocket before version 0.11.0, there is a lack of certification validation in TLS handshakes. The `Faye::WebSocket::Client` class uses the `EM::Connection#start_tls` method in EventMachine to implement the TLS handshake whenever a `wss:` URL is used for the connection. This method does not implement certificate verification by default, meaning that it does not check that the server presents a valid and trusted TLS certificate for the expected hostname. That means that any `wss:` connection made using this library is vulnerable to a man-in-the-middle attack, since it does not confirm the identity of the server it is connected to. For further background information on this issue, please see the referenced GitHub Advisory. Upgrading `faye-websocket` to v0.11.0 is recommended.

CVE-2020-15133 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **faye** - **faye-websocket** version **< 0.11.0**

CVSS3 Score: 8.7 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	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	Tags	Link
Missing TLS certificate verification · Advisory · faye/faye-websocket-ruby · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/faye/faye-websocket-ruby/security/advisories/GHSA-2v5c-755p-p4gv
Missing TLS certificate verification in Faye – The If Works	Exploit Third Party Advisory blog.jcoglan.com text/html	MISC blog.jcoglan.com/2020/07/31/missing-tls-verification-in-faye/

Related QID Numbers

180782 Debian Security Update for ruby-faye-websocket (CVE-2020-15133)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Faye-websocket Project	Faye-websocket	All	All	All	All
Application	Faye-websocket Project	Faye-websocket	All	All	All	All

cpe:2.3:a:faye-websocket_project:faye-websocket:*:*:*:*:*:*:*:*:

cpe:2.3:a:faye-websocket_project:faye-websocket:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | In faye-websocket before version 0.11.0,... | CVE-2020-15133 | Link for more: alerts.remotelyrmm.com/CVE-2020-15133	2021-11-18 20:11:29
@LinInfoSec	Ruby - CVE-2020-15133: blog.jcoglan.com/2020/07/31/mis…	2021-11-18 21:46:11

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report