

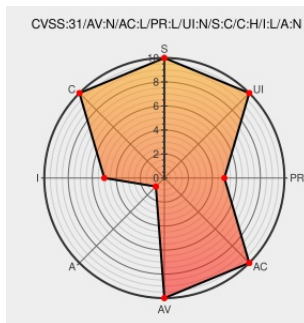


# CVE-2020-11020

Published on: 04/29/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:25 PM UTC

## CVE-2020-11020 - advisory for GHSA-qpg4-4w7w-2mq5

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

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

Faye (NPM, RubyGem) versions greater than 0.5.0 and before 1.0.4, 1.1.3 and 1.2.5, has the potential for authentication bypass in the extension system. The vulnerability allows any client to bypass checks put in place by server-side extensions, by appending extra segments to the message channel. It is patched in versions 1.0.4, 1.1.3 and 1.2.5.

CVE-2020-11020 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: faye - Faye version  $\geq 0.5.0$ ,  $< 1.0.4$

Affected Vendor/Software: faye - Faye version  $\geq 1.1.0$ ,  $< 1.1.3$

Affected Vendor/Software: faye - Faye version  $\geq 1.2.0$ ,  $< 1.2.5$

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.5 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                            | Tags                                                                                                                                                     | Link                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication and extension bypass<br>· Advisory · faye/faye · GitHub | <a href="#">Exploit</a><br><a href="#">Mitigation</a><br><a href="#">Third Party Advisory</a><br><a href="#">github.com</a><br><a href="#">text/html</a> |  CONFIRM <a href="https://github.com/faye/faye/security/advisories/GHSA-qpg4-4w7w-2mq5">github.com/faye/faye/security/advisories/GHSA-qpg4-4w7w-2mq5</a>              |
| Strict meta channel recognition in server · faye/faye@65d297d · GitHub | <a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">github.com</a><br><a href="#">text/html</a>                                 |  MISC <a href="https://github.com/faye/faye/commit/65d297d341b607f3cb0b5fa6021a625a991cc30e">github.com/faye/faye/commit/65d297d341b607f3cb0b5fa6021a625a991cc30e</a> |

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](mailto:comment@cve.report).

## Related QID Numbers

180610 Debian Security Update for ruby-faye (CVE-2020-11020)

## Known Affected Configurations (CPE V2.3)

| Type        | Vendor                       | Product              | Version | Update | Edition | Language |
|-------------|------------------------------|----------------------|---------|--------|---------|----------|
| Application | <a href="#">Faye Project</a> | <a href="#">Faye</a> | All     | All    | All     | All      |
| Application | <a href="#">Faye Project</a> | <a href="#">Faye</a> | All     | All    | All     | All      |
| Application | <a href="#">Faye Project</a> | <a href="#">Faye</a> | All     | All    | All     | All      |
| Application | <a href="#">Faye Project</a> | <a href="#">Faye</a> | All     | All    | All     | All      |

cpe:2.3:a:faye\_project:faye:\*:\*:\*:\*:node.js:\*:\*:

cpe:2.3:a:faye\_project:faye:\*:\*:\*:\*:ruby:\*:\*:

cpe:2.3:a:faye\_project:faye:\*:\*:\*:\*:node.js:\*:\*:

cpe:2.3:a:faye\_project:faye:\*:\*:\*:\*:ruby:\*:\*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

