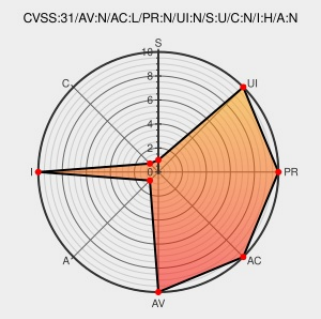
# CVE-2020-7671

Published on: 06/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:53 PM UTC

## CVE-2020-7671

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




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

goliath through 1.0.6 allows request smuggling attacks where goliath is used as a backend and a frontend proxy also being vulnerable. It is possible to conduct HTTP request smuggling attacks by sending the Content-Length header twice. Furthermore, invalid Transfer Encoding headers were found to be parsed as valid which could be leveraged for TE:CL smuggling attacks.

CVE-2020-7671 has been assigned by report@snyk.io 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 | HIGH | NONE |

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| HTTP Request Smuggling in goliath \| Snyk | Third Party Advisory snyk.io | MISC snyk.io/vuln/SNYK-RUBY-GOLIATH-569136 |

| | | |
|---|---|---|
| | text/html | |
| Issues · postrank-labs/goliath · GitHub | Third Party Advisory<br>github.com<br>text/html | MISC github.com/postrank-labs/goliath/issues/351, |

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 | Goliath Project | Goliath | All | All | All | All |

cpe:2.3:a:goliath_project:goliath:*:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→