



# CVE-2020-27813

Published on: 12/01/2020 12:00:00 AM UTC

Last Modified on: 05/14/2023 01:15:00 AM UTC

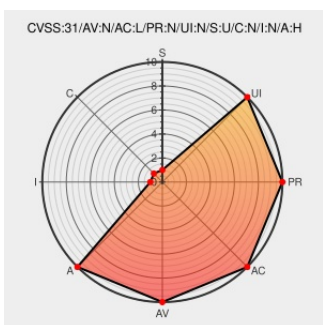
## CVE-2020-27813

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

An integer overflow vulnerability exists with the length of websocket frames received via a websocket connection. An attacker would use this flaw to cause a denial of service attack on an HTTP Server allowing websocket connections.

CVE-2020-27813 has been assigned by [secalert@redhat.com](mailto:secalert@redhat.com) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

| 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>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

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

## CVE References

| Description                                                                                 | Tags                                                                                            | Link                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Potential DoS Vector in gorilla/websocket <= v1.4.0 · Advisory · gorilla/websocket · GitHub | <a href="#">Third Party Advisory</a><br><a href="#">github.com</a><br><a href="#">text/html</a> | <b>MISC</b><br><a href="https://github.com/gorilla/websocket/security/advisories/GHSA-jf24-p9p9-4rjh">github.com/gorilla/websocket/security/advisories/GHSA-jf24-p9p9-4rjh</a> |
| [SECURITY] [DLA 3420-1] golang-websocket security                                           | <a href="#">lists.debian.org</a>                                                                | <b>MLIST</b> [debian-lts-announce] 20230513 [SECURITY]                                                                                                                         |

|                                                                                                                        |                                                                                                                                            |                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| update                                                                                                                 | <a href="#">text/html</a>                                                                                                                  | <a href="#">[DLA 3420-1] golang-websocket security update</a>                                                 |
| [SECURITY] [DLA 2520-1] golang-websocket security update                                                               | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a><br><a href="#">lists.debian.org</a><br><a href="#">text/html</a>      | <a href="#">MLIST [debian-lts-announce] 20210106 [SECURITY] [DLA 2520-1] golang-websocket security update</a> |
| 1902111 – (CVE-2020-27813) CVE-2020-27813 golang-github-gorilla-websocket: integer overflow leads to denial of service | <a href="#">Issue Tracking</a><br><a href="#">Third Party Advisory</a><br><a href="#">bugzilla.redhat.com</a><br><a href="#">text/html</a> | <a href="#">MISC bugzilla.redhat.com/show_bug.cgi?id=1902111</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

[181782](#) Debian Security Update for golang-websocket (DLA 3420-1)

[199551](#) Ubuntu Security Notification for Gorilla WebSocket Vulnerability (USN-6208-1)

[239199](#) Red Hat Update for OpenShift Container Platform 3.11.404 (RHSA-2021:0833)

[982546](#) Go (go) Security Update for github.com/gorilla/websocket (GHSA-3xh2-74w9-5vxm)

| Known Affected Configurations (CPE V2.3)      |                                |                              |         |        |         |          |
|-----------------------------------------------|--------------------------------|------------------------------|---------|--------|---------|----------|
| Type                                          | Vendor                         | Product                      | Version | Update | Edition | Language |
| Operating System                              | <a href="#">Debian</a>         | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System                              | <a href="#">Debian</a>         | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Application                                   | <a href="#">Gorillatoolkit</a> | <a href="#">Websocket</a>    | All     | All    | All     | All      |
| Application                                   | <a href="#">Gorillatoolkit</a> | <a href="#">Websocket</a>    | All     | All    | All     | All      |
| cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:  |                                |                              |         |        |         |          |
| cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:  |                                |                              |         |        |         |          |
| cpe:2.3:a:gorillatoolkit:websocket:*:*:*:*:*: |                                |                              |         |        |         |          |
| cpe:2.3:a:gorillatoolkit:websocket:*:*:*:*:*: |                                |                              |         |        |         |          |

No vendor comments have been submitted for this CVE

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)