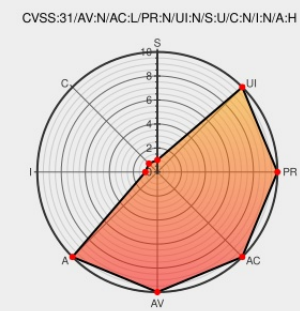
CVE-2020-27813

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 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
Potential DoS Vector in gorilla/websocket <= v1.4.0 · Advisory · gorilla/websocket · GitHub	Third Party Advisory, github.com, text/html	MISC github.com/gorilla/websocket/security/advisories/GHSA-jf24-p9p9-4rjh
[SECURITY] [DLA 3420-1] golang-websocket security	lists.debian.org	MLIST [debian-lts-announce] 20230513 [SECURITY]

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

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	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gorillatoolkit	Websocket	All	All	All	All
Application	Gorillatoolkit	Websocket	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

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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