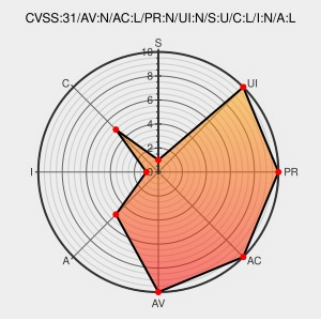
CVE-2020-8244

Published on: 08/30/2020 12:00:00 AM UTC

Last Modified on: 05/24/2022 05:31:00 PM UTC

CVE-2020-8244

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



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

A buffer over-read vulnerability exists in bl <4.0.3, <3.0.1, <2.2.1, and <1.2.3 which could allow an attacker to supply user input (even typed) that if it ends up in consume() argument and can become negative, the BufferList state can be corrupted, tricking it into exposing uninitialized memory via regular .slice() calls.

CVE-2020-8244 has been assigned by support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	LOW

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
[SECURITY] [DLA 2698-1] node-bl security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20210630 [SECURITY] [DLA 2698-1] node-bl security update
HackerOne	Exploit	MISC hackerone.com/reports/966347

Exploit
Patch
Third Party Advisory
hackerone.com
text/html

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.

Related QID Numbers

178691 Debian Security Update for node-bl (DLA 2698-1)

198527 Ubuntu Security Notification for bl Vulnerability (USN-5098-1)

982627 Nodejs (npm) Security Update for bl (GHSA-pp7h-53gx-mx7r)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bufferlist Project	Bufferlist	All	All	All	All
Application	Bufferlist Project	Bufferlist	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

cpe:2.3:a:bufferlist_project:bufferlist:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:bufferlist_project:bufferlist:*:*:*:*:*:node.js:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Debian - CVE-2020-8244: hackerone.com/reports/966347	2022-05-24 19:00:38

← Previous ID

Next ID→

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