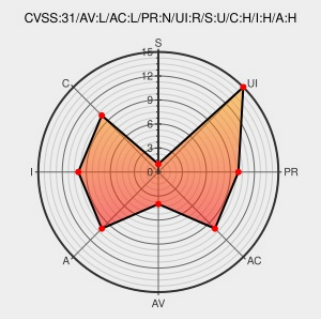
CVE-2020-29367

Published on: 11/27/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:10 PM UTC

CVE-2020-29367

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



Certain versions of C-blosc2 from C-blosc2 Project contain the following vulnerability:

blosc2.c in Blosc C-Blosc2 through 2.0.0.beta.5 has a heap-based buffer overflow when there is a lack of space to write compressed data.

CVE-2020-29367 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Fixed asan heap buffer overflow when not enough space to write compre… · Blosc/c-blosc2@c4c6470 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/Blosc/c-blosc2/commit/c4c6470e88210afc95262c8b9fcc27e30ca043ee

26442 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	Mailing List Third Party Advisory bugs.chromium.org text/html	MISC bugs.chromium.org/p/oss-fuzz/issues/detail?id=26442	

Related QID Numbers

750460 OpenSUSE Security Update for blosc (openSUSE-SU-2020:2337-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	C-blosc2 Project	C-blosc2	2.0.0	a2	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	a3	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	a4	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	a5	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta1	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta2	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta3	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta4	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta5	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	a2	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	a3	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	a4	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	a5	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta1	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta2	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta3	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta4	All	All
Application	C-blosc2 Project	C-blosc2	2.0.0	beta5	All	All

cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:a2:*:*:*:*:*:*:

cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:a3:*:*:*:*:*:*:

cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:a4:*:*:*:*:*:*:

cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:a5:*:*:*:*:*:*:

cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta2:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta3:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta4:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta5:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:a2:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:a3:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:a4:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:a5:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta1:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta2:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta3:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta4:*:*:*:*:*:*:
cpe:2.3:a:c-blosc2_project:c-blosc2:2.0.0:beta5:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→