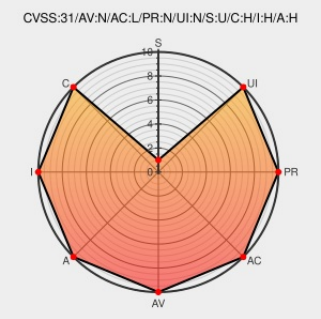
CVE-2021-4327

Published on: Not Yet Published

Last Modified on: 03/13/2023 02:10:00 PM UTC

CVE-2021-4327

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



Certain versions of Serenityos from Serenityos contain the following vulnerability:

A vulnerability was found in SerenityOS. It has been rated as critical. Affected by this issue is the function initialize_typed_array_from_array_buffer in the library Userland/Libraries/LibJS/Runtime/TypedArray.cpp. The manipulation leads to integer overflow. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The name of the patch is f6c6047e49f1517778f5565681fb64750b14bf60. It is recommended to apply a patch to fix this issue. VDB-222074 is the identifier assigned to this vulnerability.

CVE-2021-4327 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
Login required	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?ctiid.222074
LibJS: Add overflow checks when creating TypedArray from ArrayBuffer · SerenityOS/serenity@f6c6047 · GitHub	github.com text/html	MISC github.com/SerenityOS/serenity/commit/f6c6047e49f1517778f5565681fb64750b

SerenityOS - Writing a full chain exploit | devcraft.io	devcraft.io text/html	MISC devcraft.io/2021/02/11/serenityos-writing-a-full-chain-exploit.html
Login required	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?id.222074

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
Operating System	Serenityos	Serenityos	All	All	All	All

cpe:2.3:o:serenityos:serenityos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2021-4327	2023-03-01 11:38:29

← Previous ID

Next ID→