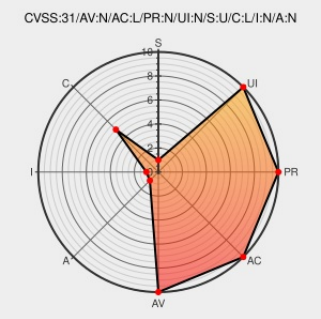
CVE-2020-36732

Published on: Not Yet Published

Last Modified on: 07/06/2023 07:15:00 PM UTC

CVE-2020-36732

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



Certain versions of Crypto-js from Crypto-js Project contain the following vulnerability:

The crypto-js package before 3.2.1 for Node.js generates random numbers by concatenating the string "0." with an integer, which makes the output more predictable than necessary.

CVE-2020-36732 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVE References

Description	Tags	Link
Native crypto module could not be used to get secure random number. · Issue #256 · brix/crypto-js · GitHub	github.com text/html	MISC github.com/brix/crypto-js/issues/256
Comparing 3.2.0...3.2.1 · brix/crypto-js · GitHub	github.com text/html	MISC github.com/brix/crypto-js/compare/3.2.0...3.2.1
Security issue · Issue #254 · brix/crypto-js · GitHub	github.com text/html	MISC github.com/brix/crypto-js/issues/254
403 Forbidden	security.netapp.com text/html Inactive Link Not Archived	CONFIRM security.netapp.com/advisory/ntap-20230706-0003/
Insecure Randomness in crypto-js | Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-CRYPTOJS-548472

Fix random number generator by evanvosberg · Pull Request #257 · brix/crypto-js · GitHub	github.com text/html	MISC github.com/brix/crypto-js/pull/257/commits/e4ac157d8b75b962d6538fc0b996e5d4d5a9466b

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
Application	Crypto-js Project	Crypto-js	All	All	All	All

cpe:2.3:a:crypto-js_project:crypto-js:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→