



# CVE-2020-36732

Published on: Not Yet Published

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

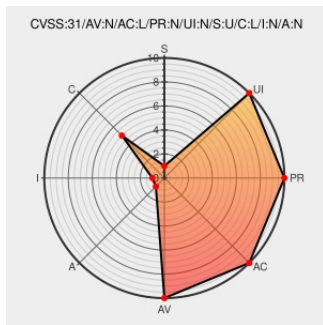
## CVE-2020-36732

[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 [M cve@mitre.org](mailto: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
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>

## CVE References

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

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](https://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](mailto: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	<a href="#">Crypto-js Project</a>	<a href="#">Crypto-js</a>	All	All	All	All
<code>cpe:2.3:a:crypto-js_project:crypto-js:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)