

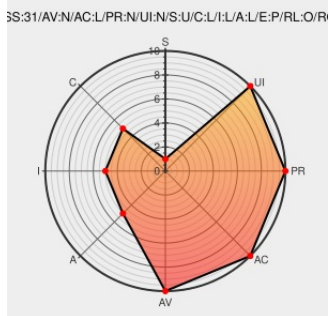


CVE-2020-7736

Published on: 10/02/2020 12:00:00 AM UTC

Last Modified on: 12/02/2022 07:47:00 PM UTC

CVE-2020-7736

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Bmoor](#) from [Bmoor Project](#) contain the following vulnerability:

The package bmoor before 0.8.12 are vulnerable to Prototype Pollution via the set function.

CVE-2020-7736 has been assigned by report@snyk.io 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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Prototype Pollution in bmoor Snyk	Exploit Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-BMOOR-598664

 [MISC github.com/b-heilman/bmoor/commit/7d4a086a1dc3ef11ed0b323824d02348734b7da5](https://github.com/b-heilman/bmoor/commit/7d4a086a1dc3ef11ed0b323824d02348734b7da5)

Related QID Numbers

Known Affected Configurations (CPE V2.3)

Discovery Credit

Social Mentions

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