

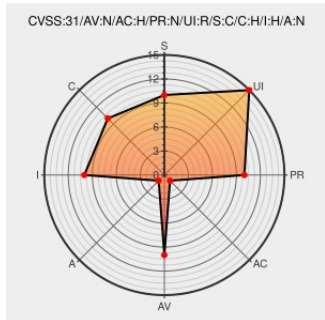


CVE-2020-26218

Published on: 11/11/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:55 PM UTC

CVE-2020-26218 - advisory for GHSA-r4w5-gw36-4792

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

Certain versions of [Touchbase.ai](#) from [Touchbase.ai Project](#) contain the following vulnerability:

touchbase.ai before version 2.0 is vulnerable to Cross-Site Scripting. The vulnerability allows an attacker to inject HTML payloads which could result in defacement, user redirection to a malicious webpage/website etc. The issue is patched in version 2.0.

CVE-2020-26218 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [puncsky](#) - [touchbase.ai](#) version < 2.0

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
HTML Injection · Advisory · puncsky/touchbase.ai · GitHub	Third Party Advisory github.com	CONFIRM github.com/puncsky/touchbase.ai/security/advisories/GHSA-r4w5-gw36-4792

