Twenty: Stored XSS via BlockNote FileBlock

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-35451
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 17:16:53 UTC
Updated	2026-04-22 21:17:23 UTC
Description	Twenty is an open source CRM. Prior to 1.20.6, a Stored Cross-Site Scripting (XSS) vulnerability exists in the BlockNote ec

Risk And Classification

Primary CVSS: v3.1 5.7 MEDIUM from security-advisories@github.com

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N

EPSS: 0.000370000 probability, percentile 0.110260000 (date 2026-04-22)

Problem Types: CWE-79 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	5.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Twentyhq	Twenty	affected < 1.20.6	Not specified

References

Reference	Source	Link
github.com/twentyhq/twenty/commit/8da69e0f77ea820a6845a4c3c025b6af3861d523	security-advisories@github.com	github.co
github.com/twentyhq/twenty/security/advisories/GHSA-7w89-7q26-gj7q	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.co
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
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 registred 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.

Free CVE JSON API cve.report/api

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