



CVE-2020-12882

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-12882
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-15 05:15:00 UTC
Updated	2020-05-19 17:15:00 UTC
Description	Submitty through 20.04.01 allows XSS via upload of an SVG document, as demonstrated by an attack by a Student against

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rcos	Submitty	All	All	All	All

References

Reference	Source	Link
[Security bug] Stored XSS Trigger for TA by user account · Issue #5266 · Submitty/Submitty · GitHub	MISC	github.com
Submitty 20.04.01 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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