



CVE-2020-35200

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-35200
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-12 18:15:00 UTC
Updated	2020-12-14 21:45:00 UTC
Description	Ignite Realtime Openfire 4.6.0 has plugins/clientcontrol/spark-form.jsp Reflective XSS.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Igniterealtime	Openfire	4.6.0	All	All	All
Application	Igniterealtime	Openfire	4.6.0	All	All	All

References

Reference	Source	Link
Openfire 4.6.0 has Reflective XSS vulnerabilities - Openfire Plugins - Ignite Realtime Community Forums	MISC	discourse.igniterealti
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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)