CVE-2020-24602

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-24602
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-02 15:15:00 UTC
Updated	2020-11-10 19:39:00 UTC
Description	Ignite Realtime Openfire 4.5.1 has a reflected Cross-site scripting vulnerability which allows an attacker to execute arbitrary

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Igniterealtime	Openfire	4.5.1	All	All	All
Application	Igniterealtime	Openfire	4.5.1	All	All	All

References

Reference
[OF-1963] Cross Site Scripting (XSS) issues - CSW Document No: C1055 CVE-2020-24601 CVE-2020-24602 CVE-2020-24604 - Ignite Realt
CVE-2020-24602 - Multiple Cross-Site Scripting (XSS) in Openfire Product
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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