



CVE-2020-27642

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

Summary

CVE	CVE-2020-27642
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-22 13:15:00 UTC
Updated	2020-10-27 19:24:00 UTC
Description	A cross-site scripting (XSS) vulnerability exists in the 'merge account' functionality in admins.js in BigBlueButton Greenlight

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bigbluebutton	Greenlight	2.7.6	All	All	All
Application	Bigbluebutton	Greenlight	2.7.6	All	All	All

References

Reference	Source
GRN2-xx: Fixed XSS vulnerability in merge user modal by farhatahmad · Pull Request #2214 · bigbluebutton/greenlight · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)