



CVE-2020-16192

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2020-16192
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-05 16:15:00 UTC
Updated	2020-08-06 19:56:00 UTC
Description	LimeSurvey 4.3.2 allows reflected XSS because application/controllers/LSBaseController.php lacks code to validate param

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Limesurvey	Limesurvey	4.3.2	All	All	All
Application	Limesurvey	Limesurvey	4.3.2	All	All	All

References

Reference	Source	Link	T
Master ls base controller check params by Shnoule · Pull Request #1479 · LimeSurvey/LimeSurvey · GitHub	MISC	github.com	P
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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