



CVE-2020-11456

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

Summary

CVE	CVE-2020-11456
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-01 16:15:00 UTC
Updated	2022-07-30 03:39:00 UTC
Description	LimeSurvey before 4.1.12+200324 has stored XSS in application/views/admin/surveysgroups/surveySettings.php and appli

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Limesurvey	Limesurvey	4.1.12	-	All	All
Application	Limesurvey	Limesurvey	4.1.12	200324	All	All
Application	Limesurvey	Limesurvey	4.1.12	-	All	All
Application	Limesurvey	Limesurvey	4.1.12	200324	All	All
Application	Limesurvey	Limesurvey	All	All	All	All

References

Reference	Source	Link
LimeSurvey 4.1.11 Cross Site Scripting ≈ Packet Storm	MISC	packet
Fixed issue [security] #16019: Stored XSS in survey groups. (Thanks t... · LimeSurvey/LimeSurvey@04b118a · GitHub	MISC	github.
LimeSurvey 4.1.11 - 'Survey Groups' Persistent Cross-Site Scripting - PHP webapps Exploit	MISC	www.e
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)