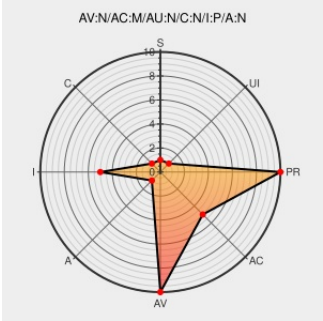
CVE-2014-5016

Published on: 07/21/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:53 PM UTC

CVE-2014-5016

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Limesurvey from Limesurvey contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in LimeSurvey 2.05+ Build 140618 allow remote attackers to inject arbitrary web script or HTML via (1) the pid attribute to the getAttribute_json function to application/controllers/admin/participantsaction.php in CPDB, (2) the sa parameter to application/views/admin/globalSettings_view.php, or (3) a crafted CSV file to the "Import CSV" functionality.

CVE-2014-5016 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Fixed issue: XSS reflection in CPDB and global settings · LimeSurvey/LimeSurvey@d23fbbd · GitHub	Exploit, Patch, github.com, text/html	CONFIRM github.com/LimeSurvey/LimeSurvey/commit/d23fbbd6c8434169967cf8bd2c5a
Lime Survey 2.05+ Build 140618 XSS / SQL Injection ≈ Packet Storm	Exploit, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/127369/Lime-Survey-2.05-Build-14061 Injection.html

comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Limesurvey	Limesurvey	2.05+	All	All	All
Application	Limesurvey	Limesurvey	2.05\+	All	All	All
Application	Limesurvey	Limesurvey	2.05\+	All	All	All

cpe:2.3:a:limesurvey:limesurvey:2.05+:*:*:*:*:*:*:*:

cpe:2.3:a:limesurvey:limesurvey:2.05\+:*:*:*:*:*:*:*:

cpe:2.3:a:limesurvey:limesurvey:2.05\+:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→