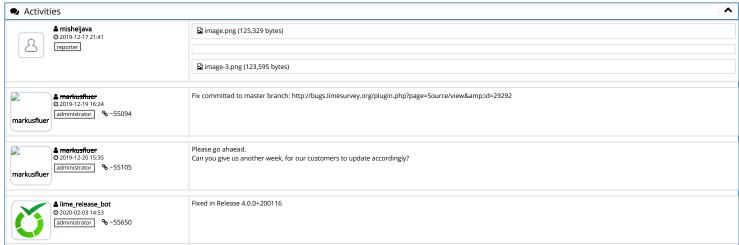
■ View Issue Details This bug affects 1 person(s). **s** 6 Category 15672 Bug reports LimeSurvey Website Reporter misheliava Assigned To Resolution Status Product 3.21.1 Version Fixed in 3.21.2 Version Summary 15672: LimeSurvey 3.21.1 Cross Site Scripting Description Title: LimeSurvey 3.21.1 Cross Site Scripting (XSS) Stored Date: 16/12/2019 Author: Guram Javakhishvili Vendor Homepage: https://www.limesurvey.org/ Software: LimeSurvey 3.21.1 Product Version: 3.21.1 Vulnerability Type: Injection Vulnerability: Cross Site Scripting (XSS) Stored LimeSurvey latest version 3.21.1 & LimeSurvey development version 4.0.0 suffer from reflective and persistent (Stored) cross site scripting and html injection vulnerabilities. Insufficient validation of user input on the authenticated part of the Limesurvey application exposes the application to persistent cross site scripting (XSS) vulnerabilities. These vulnerabilities enable potentially dangerous input from the user to be accepted by the application and then embedded back in the HTML response of the page returned by the web server. Steps To Instance 1: - (Stored Cross Site Scripting XSS vulnerabilities) Reproduce The attacker needs the appropriate permissions in order to create new Attributes. Then create an Attribute with a JavaScript payload in the Drop-down fields, for example Visit configurations > central participant database > Attributes. Now create new Attributes. Fro attribute type, select Drop-down list and click add. Now insert below XSS payload into the field and click save. (Check first image below) <svg+"/onmouseover="confirm('AttDropdown');//"onload=onload>so5cx\\"onmouseover=alert('AttDropdown');//>ciframe/onmouseover=alert('AttDropdown')></iframe>// Once saved, now click edit (see second image) Once the edit window opens it will be noted that the IFRAME has been created. When the attribute is being edited, e.g. by an administrative user, the JavaScript code will be executed in the browser. See third image below. Additional HTTP POST Request POST /limesurvey3.21.1/index.php/admin/participants/sa/editAttributeName HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0 Accept: / Accept-Language: en-GB,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 739 Origin: http://localhost Referer: http://localhost/limesurvey3.21.1/index.php/admin/participants/sa/attributeControl Cookie: LS-WIGSLIDTCJQVXTND=obtbddm0i3ddpiroojm04s8smu; LS-TRVXSHABVTHDTKHE=u56nldt5edh2rb1ljo71f3dh0o; PHPSESSID=gptp9k9bi8jcscu1ttid3pbvq8; LS-OOSUJAAJFRZHZYBG=hh6vpf8f8oomcnaqc03h2qcpdm; YIL_CSf YII_CSRF_TOKEN=eGthZG9JTGZ1d2RHcHk3bGUyT1R5X1pCOHd5Nkp5eFMG8IWciXbJNQCd-EOnoJN1jIMWEo3pj4aYbFBa-FAXIA%3D%3D&oper=edit&ParticipantAttributeName%5Battribute_id%5D=1&ParticipantAttributeName%5Bdefaultname%5D=test&ParticipantAttributeName%5Battribute_type%5D=DD&ParticipantAttributeName%5Bvisible%5D Tags No tags attached. **Bug heat** 6 limesurvey3.21.1+191210 Complete LimeSurvey version number (& build) I will donate to the project if issue is Browser Chrome & Firefox

t .	
Database type & version	DB Server version: 10.4.6-MariaDB Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407
Server OS (if known)	
Webserver software & version (if known)	
PHP Version	PHP version: 7.3.9





Related Changesets	Related Changesets				
② 2019-12-19 16:23:08	Fixed issue 15672 : LimeSurvey 3.21.1 Cross Site Scripting	Affected Issues 15672			
a markusfluer Details Diff	mod - application/views/admin/participants/modal_subviews/_editAttribute.php	Diff File			

೨ Issue History					
Date Modified	Username	Field	Change		
2019-12-17 21:41	misheljava	New Issue			
2019-12-17 21:41	misheljava	File Added: image.png			
2019-12-17 21:41	misheljava	File Added: image-2.png			
2019-12-17 21:41	misheljava	File Added: image-3.png			
2019-12-19 10:44	cdorin	Assigned To	=> markusfluer		
2019-12-19 10:44	cdorin	Status	new => assigned		
2019-12-19 16:24	markusfluer	Changeset attached	=> LimeSurvey master 38e1ab06		
2019-12-19 16:24	markusfluer	Note Added: 55094			
2019-12-19 16:24	markusfluer	Resolution	open => fixed		
2019-12-19 16:25	markusfluer	Status	assigned => resolved		
2019-12-19 16:25	markusfluer	Fixed in Version	=> 3.21.2		
2019-12-20 15:35	markusfluer	Note Added: 55105			
2020-02-03 14:53	lime_release_bot	Note Added: 55650			
2020-02-03 14:53	lime_release_bot	Status	resolved => closed		
2020-05-04 09:43	ollehar	View Status	private => public		
2020-05-04 09:43	ollehar	Description Updated			
2020-05-04 09:43	ollehar	Steps to Reproduce Updated			
2020-05-04 09:43	ollehar	Additional Information Updated			