security-assessment.com

Vulnerability Advisory

Name	BlackBerry Enterprise Service 12 (BES12) Self-Service
Vendor Website	www.blackberry.com
Date Released	15 Feb 2016
Affected Software	BES12 before 12.4
Researchers	Adrian Hayes

Description

Blackberry BES12 is an enterprise mobile management solution and contains a self-service web application available to mobile users. This web application contains multiple vulnerabilities including unauthenticated SQL injection and reflected cross site scripting.

Limited access to an on-premise BES12 environment was provided during the discovery of these vulnerabilities. The full impact of the vulnerabilities in relation to compromising other portions of the BES12 solution, such as mobile devices, is unclear.

Exploitation

SQL Injection

The Java servlet *com.rim.mdm.ui.server.ImageServlet* is vulnerable to SQL injection via the *imageName* parameter. This servlet is exposed at multiple paths and is used to fetch an image from the database:

URL Path	Parameter
/mydevice/client/image	imageName
/admin/client/image	imageName
/myapps/client/image	imageName
/ssam/client/image	imageName
/all/client/image	imageName

This was discovered on a production BES12 on-premise deployment and the injection vector allowed both UNION and stacked queries to be executed on the Microsoft SQL server used by BES12. This allows full read/write access to the database, and can potentially result in command execution via xp_cmdshell depending on the database user configuration.

The following proof of concept demonstrates an injection payload which will select the entire obj_keystore_entry table. The query will serialise the entire table into an XML document which is returned in the HTTP response as UTF-16 without the leading BOM (byte order mark) causing most text editors to fail to display the response correctly.

Proof of Concept – UNION Injection

```
https://<server>/mydevice/client/image?imageName=ui.cobranded.login.
logo'+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,(SELECT+*+FROM+obj_keystore_entry+FOR+XML
+PATH(''))+--
```

The technique above can be used to download any database table available to the BES12 database user.

Notable database tables are:

- *obj_user* which contains BES12 user details.
- *obj_user_authentication* which contains authentication tokens.
- *obj_user_device* which based on column names, contains enrollment tokens, enrollment secrets and device encryption keys.

It is unclear if this information is sufficient to decrypt a lost/stolen BES12 mobile device.

Reflected Cross Site Scripting

Two areas of the self-service web application exist where user-supplied input is reflected directly in web pages, allowing a malicious user to conduct Cross Site Scripting (XSS) attacks against users of the application. While the application uses the HttpOnly cookie flag for session tokens, successful exploitation allows malicious JavaScript to perform any action within the application that the targeted user is able to. The administrative web application is typically hosted on the same domain and may be attacked using these XSS vectors, although this is BES12 deployment specific.

The table below details where Cross Site Scripting was detected and which parameters are vulnerable:

URL Path	Parameter	POC Payload
/mydevice/index.jsp	locale	/mydevice/index.jsp?locale="><script>alert(1)</script>
/mydevice/loggedOut.jsp	locale	/mydevice/loggedOut.jsp?locale="><script>alert(1)</script>

The following screenshot displays an HTML response showing injected JavaScript content:

Cross Site Scripting - HTTP Response

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.
<html lang="decdcel"><script>alert(1)</script>a5dfd">
<head>
    <!-- 3/10 -->
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta http-equiv="content-type" content="text/html; ch



        <title>BES12 Self-Service</title>
```

Solution

Upgrade to BES12.4.

Timeline

Initial disclosure to Blackberry – 19 Nov 2015
Disclosure receipt confirmed by Blackberry – 19 Nov 2015
Request for update from Blackberry – 7 Dec 2015
Vulnerabilities confirmed by Blackberry – 8 Dec 2015
Blackberry confirms fixes will be released as part of BES12.4 – 28 Jan 2016
BES12.4 released – 29 Jan 2016
Advisory released – 15 Feb 2016

About Security-Assessment.com

Security-Assessment.com is a 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