Blackberry World Vulnerable to MiTM

15/10/14

Software:	Blackberry 10, Blackberry World
Affected Versions:	OS version 10.3.0 - BlackBerry World versions earlier than 5.1.0.53 OS version 10.2.1 - BlackBerry World versions earlier than 5.0.0.263 OS version 10.2.0 - BlackBerry World versions earlier than 5.0.0.262
CVE Reference:	CVE-2014-6611 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6611) BSRT-2014-008 CVSS Score 4.3
Author:	Henry Hoggard - MWR Labs (https://labs.mwrinfosecurity.com/)
Severity:	High
Vendor:	Blackberry
Vendor Response:	http://www.blackberry.com/btsc/KB36360

Description:

The Blackberry World application on Blackberry 10 is vulnerable to a Man-in-The-Middle (MiTM) attack. Blackberry World is Blackberry's official marketplace application and is installed by default on all Blackberry 10 devices.

A vulnerability exists in the BlackBerry World services download mechanism, which is used by the BlackBerry World application on affected BlackBerry 10 smartphones.

BlackBerry World allows users to search for and download apps for their BlackBerry device. An attacker, utilising a Man-in-The-Middle (MiTM) attack, could intercept a user's BlackBerry World application download and, as a result, install malware on the device.

Successful exploitation of this vulnerability could result in an attacker gaining access to any data or settings that are accessible through the permissions that the user accepted when installing the malicious application.

In order to exploit this vulnerability, an attacker must intercept a user's application download/update request from BlackBerry World over a compromised network and replace the response from the server with a malicious file. The user must then accept the application permissions and install the malicious application.

Impact:

If the requirements are met for exploitation, an attacker could potentially gain access to any data or settings allowed by the application permissions that the user granted for the installed application.

Cause:

Blackberry World uses a clear text communication channel (HTTP) for most of its requests, this allows attackers to intercept and modify the data being sent and received. An attacker could replace application code as it traverses the network with code of the attackers choosing.

Interim Workaround:

Users should download or update applications only while they are connected to trusted networks. Users should also pay particular attention to the permissions requested by applications to ensure they are appropriate for the applications purpose. Careful considerations should be given to which application permission settings to grant or deny whenever installing applications from BlackBerry World.

Solution:

All BlackBerry World downloads are now protected by SSL encryption, which helps mitigate the risk to those running affected versions, including on BlackBerry 10 OS versions earlier than 10.2.0.

A software update resolves this vulnerability on affected versions of BlackBerry 10 smartphones. The update is made available automatically on affected devices via the BlackBerry Hub.

A version of BlackBerry World, that does not contain the reported vulnerabilities, can be downloaded manually by visiting www.mobile.blackberry.com from a BlackBerry device or by visiting www.blackberry.com/blackberryworld from a computer.

Technical details

Blackberry World uses a clear text communication channel (HTTP) for most of its requests allowing attackers to intercept and modify the data being sent and received.

Presented below is an example request that is sent when requesting an application for installation. The request is sent to the host download.appworld.blackberry.com on TCP Port 80 using HTTP.

```
GET /ClientAPI/file2/27215757?dwnAuth=1397209102_0c1e2939deb480abcd6e8cea73009e9d HTTP/1.1
Accept-Language: en_GB
Content-Language: en_GB
Content-Type: application/x-www-form-urlencoded
User-Agent: AppWorld/5.0.0.131
Connection: Keep-Alive
Accept-Encoding: gzip
Host: download.appworld.blackberry.com
```

This behaviour was witnessed during application update requests as well as installation requests. Therefore it is possible to intercept and modify applications at installation and if an update of an existing application is attempted.

Blackberry states “BlackBerry World employs application integrity checking and secure download methods to ensure that the correct application is downloaded and installed”. The server response includes two sha512 hashes that are used to validate the integrity of the page. If the page is modified the application hashes will not match and the application will error and exit. However this is easily bypassed if the hashes are removed from the response entirely. An example response is presented below to illustrate the presence of the removable headers (X-APPWORLD-SIG and X-APPWORLD-SIG-SHA512).

```
HTTP/1.1 200 OK
Server: Apache
X-Powered-By: RIM
X-APPWORLD-MIN: 5.0.0.129
X-PAYMENTSDK-MIN: 1.0
X-APPWORLD-VER: 10.2.172.22
X-CLIENT-CONFIG-VERSION: 4
X-CLIENT-DATA-VERSION: 1
X-PAYMENT-CONFIG-VERSION: 31
X-PAYMENT-DATA-VERSION: 1
X-PAYMENTURLS-CONFIG-VERSION: 2
X-CLIENT-CACHE-TIME: 900000
X-APPWORLD-SIG:
F75aCGzyrL8H1P5BgVa1xIgoMZ67/E6OhuM9QdXMi64uyDvcYrdY8bwUTncB1dEblTyWC8cXSZ7OqJWbBrIeiom0dLcF+j
mtp2Kaz5CZ9evaiZKVF3zvT9xsDEaTq05U2ZYeT8T+8hswipjUoDqSWWwgiVYYyxmXZm1LNNmkhEg=
X-APPWORLD-SIG-SHA512:
CoyAOhyQvhJHen5QvDdcnl3OOQ200e2JGgCiIcKhv92Pe4UnSj9K0MlxnmhGrjGrP9CwudkQpJcAbfGI/d9olH9fomVqPu
UHSQ5rMbXyE/MlnoBl08Ng1i9Mpr1+XyOGFOsBzm+SS8r08MVFoDsbqExvH+YmGgvtosyglo8loPc=
Content-Length: 11072
Content-Type: text/xml;charset=UTF-8
Cache-Control: max-age=21554
Date: Fri, 11 Apr 2014 09:07:15 GMT
Connection: keep-alive
```

Detailed Timeline

Date:	Summary:
16/04/2014	Vulnerability reported to Blackberry
16/04/2014	Blackberry acknowledged advisory
28/04/2014	Blackberry confirmed vulnerabilities
25/09/2014	MWR notified that a patch was to be made available on 14/10/2014
14/10/2014	Blackberry published advisory (BSRT-2014-008)
16/10/2014	MWR published advisory