RIM Customer Statement Regarding Etisalat / SS8 Software

Updated: July 17, 2009

Recently, Etisalat, a carrier in the United Arab Emirates (UAE), sent an SMS message to a number of their customers informing them of a software patch that was available for BlackBerry smartphones and indicating that the software patch would enhance the performance of the BlackBerry service if it was downloaded and installed on the smartphone. Etisalat included a web link in the SMS message urging these customers to download and install the software.

Etisalat also issued a press release that referred to the software as a BlackBerry Software Upgrade.

RIM confirms that this software is not a patch and it is not a RIM authorized upgrade. RIM did not develop this software application and RIM was not involved in any way in the testing, promotion or distribution of this software application.

RIM further confirms, in general terms, that a third party patch cannot provide any enhancements to network services as there is no capability for third parties to develop or modify the low level radio communications protocols that would be involved in making such improvements to the communications between a BlackBerry smartphone and a carrier's network.

In addition, RIM is not aware of any technical network concerns with the performance of BlackBerry smartphones on Etisalat's network in the UAE. In situations where there is a need to upgrade the firmware on a BlackBerry smartphone to address network performance issues, RIM distributes official BlackBerry software updates through standard channels, including direct downloads from BlackBerry.com and over-the-air software updates using the built in Wireless Upgrade feature of the BlackBerry smartphone. RIM does not use SMS or WAP push as an official distribution channel for these types of official BlackBerry software updates.

In this case, Etisalat appears to have distributed a telecommunications surveillance application that was designed and developed by SS8. In order to install and successfully run this application, a user would need to click on the link to the web site and then confirm their intent to download the software and provide their explicit authorization for the application to access network resources. Under such circumstances, independent sources have concluded that it is possible that the installed software could then enable unauthorized access to private or confidential information stored on the user's smartphone.

Note: RIM does not endorse this software application and, if a user installed the software application, it can be subsequently removed from the user's smartphone as described below.

RIM would like to remind our customers that all smartphones can be utilized as multifaceted application platforms that enable their owners to chose and install a wide range of applications to suit their needs from a large number of third party developers, but careful consideration should be given when determining which applications are allowed to be installed by the user on their device. The BlackBerry platform has a number of built-in security measures that require the smartphone user to explicitly agree to install and authorize an application.

In general, all users (of any type of computing device, from any manufacturer) should avoid downloading and installing applications from unknown or untrusted sources. Organizations that have deployed the BlackBerry Enterprise Server can use the IT policy and application control settings to prevent or safe-guard against a user downloading and installing unauthorized applications on a BlackBerry smartphone. In addition, the BlackBerry Enterprise Server software allows administrators to also limit what resources are accessible by an application running on a BlackBerry smartphone.

The IT policy settings for preventing the installation and execution of unauthorized applications on a BlackBerry smartphone can be remotely set by the administrator. Additional measures can be taken by installing the BlackBerry Enterprise Solution in a segmented network. RIM's customers can reference the following documents for a detailed description of the capabilities that are inherent in the platform:

Placing the BlackBerry Enterprise Solution in a segmented network (PDF)
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/1181821/828044/1181292/Placement_of_the_BlackBerry_Enterprise_Solution_in_a_Segmented_Network.pdf?nodeid=1265885&vernum=0

Protecting the BlackBerry device platform against malware (PDF)
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/1181821/828044/1181292/Protecting_the_BlackBerry_device_platform_against_malware.pdf?nodeid=1266119&vernum=0

Additional Questions and Answers:

Q. How can an application written for a BlackBerry smartphone be installed?

There are only five ways an application can be installed on a BlackBerry smartphone:

1.   BlackBerry AppWorld

2.   Application loader though the Desktop Manager

3.   Apploader Lite

4.   Wireless Application Push from your BES Administrator. Note that only BES Administrators can push applications directly to BlackBerry smartphones on their network; RIM and Wireless Operators cannot remotely install applications in this manner.

5.   JAD Download link
     a.   This download link can be provided though an email, IM, SMS, PIN, or web page
     b.   If a user clicked the link, they would be asked questions on the smartphone to confirm the following:
          * Would you like to download the application?
          * Do I trust the application?

Q. How can we determine if this application was installed on our smartphones?

On the smartphone, the user can perform the following steps:

From the Options screen:
- Select Advanced Options

- Select Applications

- From the menu, select Modules

If the user sees a module named "Registration" listed, the user can click on the module to see if it has the following characteristics:

Type:	Application
Title:	Registration
Description:	Etisalat network upgrade for BlackBerry service.
	Please download to ensure continuous service quality.
Version:	4.9100
Size:	19140 Bytes
Created:	July 4, 2009 12:51
Vendor:	Etisalat
Applications:	Registration
Hash:	C8AE A07D A288 74F0 A08B
	1315 8849 4E8D 4908 7D3C

Note: some of these values may change if the user has installed a different revision of this software.

From the BES, the administrator also has the following options:

1) The BlackBerry Resource Kit has a tool called 'HHAppReport'. This will allow the administrator to build a report for all users and all applications each user has installed.

    To obtain the BRK and the documentation, view the following:
    http://na.blackberry.com/eng/support/server_resourcekit.jsp#tab_tab_components

2) BES administrators can execute the following query against their BES database in order to determine if any of their users have installed the "Registration" software from Etisalat:

```
SELECT SyncDeviceMgmt.UserConfigID, SyncDeviceMgmt.ModuleName,
UserConfig.PIN, UserConfig.DisplayName
FROM SyncDeviceMgmt
INNER JOIN UserConfig
ON SyncDeviceMgmt.UserConfigID=UserConfig.Id
WHERE SyncDeviceMgmt.ModuleName='Registration'
```

This will provide a list of impacted devices. You can then use this information to contact the relevant users and provide the appropriate removal instructions.

Q. How does this application work? How is it activated by the wireless provider?

RIM recommends that you contact Etisilat or SS8 directly for information on how this software is administered. RIM did not develop or deploy this application and cannot provide any details on the operation of this software.

RIM does not have a partnership with SS8 and does not endorse the development of this type of software for any platform.

Q. How is the "Registration" program installed on a user's smartphone?

Etisalat originally sent an SMS message with a link to a web site where the "Registration" program could be downloaded.

Warning: Please also be aware that an SMS message could **potentially** be sent again suggesting that users need to click on a link to remove the application, but the link in the subsequent SMS message **could** actually lead to the same application (or an update to the application).

Once the "Registration" program is downloaded, it begins to execute, the user is prompted to allow the application to have network access via HTTP. If the user allows the application to have network access, it will run discretely in the background. There is no further user interaction required as the application appears to be intentionally designed to run in the background with no user interaction or visibility.

If network access is not authorized, the application may run in the background but will not be able to receive administration commands from Etisalat and will not be able to send data back to Etisalat's servers. However, it appears that all BlackBerry software functionality would continue to run normally.

If your BES administrator has set policies controlling the use of applications or preventing users from downloading applications, then the user will not be able to download this software.

Q. Can this application be un-installed? If so, how can this be accomplished from the server and the smartphone.

To remove the application from a BlackBerry smartphone using the BES, the following steps can be taken. Note that this will remove all third party applications and will require that users reload any properly authorized applications onto their BlackBerry smartphones.

Removing all 3rd party applications from a user's smartphone through the BES.

First create a software configuration.

1) In the BlackBerry® Administration Service, on the BlackBerry solution management menu, expand Software.

2) Click Create a software configuration.

3) In the Configuration information section, in the Name field, type a name for the software configuration.

4) In the Disposition for unlisted applications drop-down list, perform the following action:

   a. To prevent users from installing applications that are not included in the software configuration on their BlackBerry smartphones, click Disallowed.

5) In the Application control policy for unlisted applications drop-down list, click the application control policy for unlisted applications that you want to assign to the software configuration.

6) Click Save.

Assign a software configuration to a group

1) In the BlackBerry® Administration Service, on the BlackBerry solution management menu, expand Group.

2) Click Manage groups.

3) Click a group.

4) Click Edit group.

5) On the Software configuration tab, in the Available software configurations list, select the software configuration created above.

6) Click Add.

7) Click Save all.

To remove the "Registration" application from the smartphone, there are multiple approaches that can be used:

1) Using the javaloader.exe utility on your desktop PC:

   a. Download and install the [BlackBerry Java Development Environment Component Package](#) (6.5 MB).
   b. Connect your BlackBerry smartphone to a desktop via the USB cable.

   c. Remove the application using Javaloader by issuing the following command:

      javaloader -u erase –f Registration.cod

      If prompted, enter the device password on your desktop computer.

2) Directly from your smartphone:

   a. Download the RemoveRegistration application from the following link:

      www.blackberry.com/registrationappremover

   b. When prompted, begin the download and authorize the application to run.

   c. The application will run and if the Registration.cod file exists on your smartphone it will be deleted. Note that your smartphone may need to reset in order to complete this operation.

Q. I am having trouble removing the "Registration" application, how can I disable this application?

During the install process, the user may have granted permission for the application to access all of the data on the device and to connect to network resources

1. Navigate to Options/Advanced Options/Applications.
2. Select Modules from the menu.
3. Scroll until you find Registration.
4. Select Edit Permissions from the menu.
   1. Scroll to Connections and select Change Option. Change the selection from Allow to Deny.
   2. Scroll to Interactions and select Change Option. Change the selection from Allow to Deny.
   3. Scroll to Connections and select Change Option. Change the selection from Allow to Deny.

The BlackBerry smartphone may ask you to reboot, click yes and allow the smartphone to reset.

Changing these permissions and rebooting your BlackBerry smartphone will effectively disable this application by preventing it from accessing any information on your device or connecting to any network resources.

Q. How can we prevent / lock down future types of these applications from being installed on our users' devices via IT policy without affecting current functionality?

This can be accomplished through the Application Control Policy from the BlackBerry Enterprise Server using one of the following methods

1) Using Software Configurations, Create a white list for your applications (Disable all 3rd party applications and allow every authorized application specifically).

2) Using a software configuration add each unwanted application to the software configuration and set the disposition of the Application Control Policy to Disallow.

For more info on how to control and remove third party applications please see:
http://www.blackberry.com/btsc/KB05392

Q. How can I protect against unwanted applications in general?

There are several unique IT Polices, and Application Control policies that can help restrict, or block 3rd party applications. For more info please view the following:

http://na.blackberry.com/eng/ataglance/security/it_policy.jsp

http://na.blackberry.com/eng/deliverables/7229/Application_control_policy_rule_descriptions_325050_11.jsp

Q. Where can I find more information about how to protect against unwanted applications on my users' BlackBerry Smartphones?

The following white papers provide additional information to help you understand how to effectively manage the risks associated with malware and other unwanted applications:

Protecting the BlackBerry device and BlackBerry Enterprise Server against malware
http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB05499

Placing the BlackBerry Enterprise Solution in a segmented network (PDF)
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/1181821/828044/1181292/Placement_of_the_BlackBerry_Enterprise_Solution_in_a_Segmented_Network.pdf?nodeid=1265885&vernum=0

Protecting the BlackBerry device platform against malware (PDF)
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/1181821/828044/1181292/Protecting_the_BlackBerry_device_platform_against_malware.pdf?nodeid=1266119&vernum=0

Q. How can I be sure that I have only the factory authorized software on my smartphone?

If you want to return your smartphone to the original state with only RIM original, authorized software loaded on the smartphone you can perform the following steps. Please note, that you may want to back up your personal data and and any **trusted** applications on your smartphone as this process will remove all data and third party applications.

- Select the wipe handheld option from the appropriate menu to delete all content on the smartphone
- Download the latest BlackBerry smartphone software from your wireless service provider.
- Install/upgrade the software using the BlackBerry Desktop Manager

Further instructions on preparing a BlackBerry smartphone for resale or purchasing a used BlackBerry smartphone can be found at:

http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB05099&sliceId=2&docTypeID=DT_SUPPORTISSUE_1_1&dialogID=121884049&stateId=0%200%20121872547

For more information, visit www.blackberry.com/security