IC-IRC

Intelligence Community Incident Response Center

(U) IC-IRC Situational Awareness Report

(U//FOUO) Situational Awareness reports contain information on a variety of issues such as general information reports, quarterly/semi-annual/annual summaries, isolated communications outages, other information of value to the IC.

(U) Vulnerabilities in Blackberry® Enterprise Server Could Allow Remote Code Execution

Date: 18 February 2013
TRACKING NUMBER: ICIRC-SA-022-2013

(U) SUMMARY

(U) Vulnerabilities exist in components of the BlackBerry® Enterprise Server (BES) that processes images for rendering on BlackBerry® smart phones. An attacker could exploit these vulnerabilities to execute remote code to achieve privileged access to the BlackBerry® Enterprise Server and potentially access other portions of the Enterprise network. Patches and workarounds are currently available. Research in Motion (RIM), the BlackBerry® parent company, states that exploits for this vulnerability have yet to be observed in the wild targeting these vulnerable BlackBerry® components. These vulnerabilities do not affect any BlackBerry® smart phones or the BlackBerry® Device Software.

(U) DETAILS

(U) Vulnerabilities exist in the following components of the BlackBerry® Enterprise Server Express for Microsoft Exchange, IBM Lotus Domino, and Novell Groupwise version 5.0.4 and earlier:

- **BlackBerry® Mobile Data System (MDS) – Connection Service**: Processes images on web pages that the BlackBerry® Browser requests.
- **BlackBerry® Messaging Agent**: Processes images in email messages.
- **BlackBerry® Collaboration Service**: Processes images in instant messages sent between an organization's instant messaging server, its BlackBerry® Enterprise Server, and devices that are using public APIs.

(U) The vulnerabilities exist in the libtiff library utilized by the components above to process and display Tagged Image File Format (TIFF) images. A TIFF file is composed of small descriptor blocks containing offsets into the file which point to a variety of data types. Incorrect offset values can cause programs to attempt to read erroneous portions of the file or attempt to read past the physical end of file. Improperly encoded packet or line lengths within the file can cause rendering programs which lack appropriate boundary checks to overflow their internal buffers.

(U) The vulnerability in the BlackBerry® MDS – Connection Service requires action from the victim to click a link for the exploit to work. An attacker could send this link to a BlackBerry® user through a website, an email, or an instant message. Once the user clicks the link, the BlackBerry® MDS Connection Service would process the malformed TIFF file and the attacker could potentially compromise the BlackBerry® Enterprise Server and gain privileged access.

(U) The vulnerabilities in the BlackBerry® Messaging Agent and Collaboration Service do not require the same user input to exploit. An attacker could send a malformed TIFF file in an email or an instant message and the Messaging Agent or Collaboration Service would attempt to render the TIFF thereby executing the exploit.

(U) Successful exploit of any of these vulnerabilities could enable an attacker to execute code on the BlackBerry® Enterprise Server with the permissions of the service account used to start the BlackBerry® Enterprise Server service. If the service account is improperly configured or has permissions and privileges that it should not have, the attacker could potentially execute a privilege escalation and achieve administrator or system level access. This could enable an attacker to move laterally across the Enterprise to other resources.

(U) The vulnerabilities in the BlackBerry® Enterprise Server are related to the vulnerabilities identified in CVE-2012-2088 and CVE-2012-4447.

(U) MITIGATING FACTORS

(U) RIM has released a patch, BlackBerry® Enterprise Server 5.0.4 MR2 to address and mitigate these vulnerabilities. Additionally, RIM has released an interim security update that patches these vulnerabilities but does not contain other changes and updates included with the BlackBerry® Enterprise Server 5.0.4 MR2 patch. Both fixes can be downloaded from the BlackBerry® website here: http://www.BlackBerry®.com/go/serverdownloads.

(U) The IC-IRC recommends all elements that are using affected versions of the BlackBerry® Enterprise Server software, install the 5.0.4 MR2 patch or the interim security update as soon as possible to prevent the exploit and compromise of your system. If you are unable to implement the patches, RIM has also provided the below workarounds to prevent the vulnerable library from being used to render and display TIFF images.

(U) Prevent the BlackBerry® Enterprise Server from using the vulnerable image.dll file when processing images using the BlackBerry® MDS Connection Service

(U) Change the BlackBerry® MDS Connection Service settings in the rimpublic.property file to turn off image processing that uses the vulnerable image.dll file.

1. Navigate to the rimpublic.property file (for example, C:\Program Files\Research In Motion\BlackBerry® Enterprise Server\MDS\Servers\instance\config\rimpublic.property).
2. In a text editor, open the rimpublic.property file.
3. Add the following settings to the rimpublic.property file:
   ```
   application.handler.rim.slipstream.clientless=false
   application.handler.rim.slipstream.clientful=false
   application.handler.rim.slipstream.progressive=false
   ```
4. Save and close the rimpublic.property file.

(U) Note: When the workaround for the BlackBerry® MDS Connection Service is implemented customers will still see inline images in messages. The workaround causes the BlackBerry® MDS Connection Service to use a non-vulnerable library for image processing.

(U) Prevent the BlackBerry® Enterprise Server from using the vulnerable image.dll file when processing images using the BlackBerry® Collaboration Service

(U) Change the BlackBerry® Collaboration Service settings in the rimpublic.property file to turn off image processing that uses the vulnerable image.dll file.

1. Navigate to the rimpublic.property file (for example, C:\Program Files\Research In Motion\BlackBerry® Enterprise Server\BBIM\Servers\instance\config\rimpublic.property).
2. In a text editor, open the rimpublic.property file.
3. Add the following settings to the rimpublic.property file:
   ```
   application.handler.rim.slipstream.clientless=false
   application.handler.rim.slipstream.clientful=false
   application.handler.rim.slipstream.progressive=false
   improxy.slipstream=false
   ```
4. Save and close the rimpublic.property file.

(U) Note: When the workaround for the BlackBerry® Collaboration Service is implemented customers will still see inline images in instant messages. The workaround causes the BlackBerry® Collaboration Service to use a non-vulnerable library for image processing.

(U) Prevent the BlackBerry® Enterprise Server from processing inline images using the BlackBerry® Messaging Agent

For BlackBerry® Enterprise Server 4.1:

1. In the left pane of BlackBerry® Manager, select a BlackBerry® Enterprise Server.
2. On the Server Configuration tab, click **Edit Properties**.
3. Click **Messaging**.
4. In the Messaging Options section, perform one of the following actions:
    - To turn on rich content formatting, click **Rich Content Enabled**. In the drop-down list, click **True**.
    - To turn on inline images, click **Inline Images Enabled**. In the drop-down list, click **True**.
5. Click **OK**.

For BlackBerry® Enterprise Server 5.0:

1. In the **BlackBerry® Administration Service**, under **Servers and components**, expand **BlackBerry® Solution Topology** > **BlackBerry® Domain** > **Component View** > **Email**
2. Click the name of the BlackBerry® Enterprise Server instance
3. Click **Edit instance**.
4. On the **Messaging** tab, perform one or both of the following options:
    - To turn off rich text formatting, in the Messaging Options section, change **Rich content turned on** to **False**.
    - To prevent sending inline images, in the Messaging Options section, change **Automatic downloading of inline images turned on** to **False**.
5. Click **Save All**.

(U) REFERENCES/RELEVANT URLs and/or SOURCES

BlackBerry® Knowledge Base Article KB33425, Accessed February 17, 2013
http://btsc.webapps.BlackBerry®.com/btsc/viewdocument.do?externalId=KB33425&sliceId=1&cmd=displayKC&docType=kc&noCount=true&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl

BlackBerry® Knowledge Base Article KB15931, Accessed February 17, 2013
http://btsc.webapps.BlackBerry®.com/btsc/viewdocument.do?externalId=KB15931&sliceId=2&cmd=displayKC&docType=kc&noCount=true&ViewedDocsListHelper=com.kanisa.apps.common.BaseViewedDocsListHelperImpl

Common Vulnerabilities and Exposures – CVE-2012-2088, Accessed February 17, 2013
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2088

Common Vulnerabilities and Exposures – CVE-2012-4447, Accessed February 17, 2013
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-4447

Wikipedia – Libtiff, Accessed February 17, 2013 http://en.wikipedia.org/wiki/Libtiff

Wikipedia – Tagged Image File Format (TIFF), Accessed February 17, 2013
http://en.wikipedia.org/wiki/Tagged_Image_File_Format

National Vulnerability Database - CVE-2012-2088
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2088

(U) FEEDBACK INSTRUCTIONS

(U) None at this time.

(U) IC-IRC CONTACT INFORMATION

(U//FOUO) Intelligence Community Incident Response Center (IC-IRC)
Secure: 984-6371 ♦ Comm: 202-231-8900
STE: 202-231-8900 ♦ DRSN: 228-7424
ICIRC@dodiis.ic.gov
http://intelshare.intelink.ic.gov/sites/icirc/default.aspx