

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

8/10/2011

SUBJECT:

Vulnerabilities in BlackBerry Enterprise Server Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the BlackBerry Mobile Data System (MDS) Connection Service and BlackBerry Messaging Agent that could allow remote code execution on the affected BlackBerry Enterprise Server. The MDS Connection Service is used to provide wireless application management across mobile devices. The BlackBerry Messaging Agent is used to provide wireless messaging services to mobile devices. Exploitation of these vulnerabilities could result in the attacker gaining the same privileges as the BlackBerry Enterprise Server service account. Depending on the privileges associated with the account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- BlackBerry Enterprise Server version 5.0.1 through 5.0.3 MR2 for Microsoft Exchange
- BlackBerry Enterprise Server version 5.0.1 through 5.0.3 MR2 for IBM Lotus Domino
- BlackBerry Enterprise Server version 4.1.7 and version 5.0.1 through 5.0.1 MR3 for Novell GroupWise
- BlackBerry Enterprise Server Express version 5.0.1 through 5.0.3 for Microsoft Exchange
- BlackBerry Enterprise Server Express version 5.0.2 and 5.0.3 for IBM Lotus Domino

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:

Multiple vulnerabilities have been discovered in the BlackBerry MDS Connection Service and the BlackBerry Messaging Agent on the BlackBerry Enterprise Server.

The MDS Connection Service vulnerability can be exploited if a user browses to a specially crafted web page. This could occur by following a link an attacker has sent in an email or through instant messenger.

The Messaging Agent vulnerability can be exploited if an attacker creates a message containing specially crafted PNG and TIFF images and sends the message to a BlackBerry smartphone user. The user does not need to click a link, open an image, or view the email message for the attack to succeed.

Successful exploitation of either vulnerability could result in the attacker gaining the same privileges as the BlackBerry Enterprise Server service account. Depending on the privileges associated with the account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Research in Motion to vulnerable systems immediately after appropriate testing.
- Apply the principle of least privilege to all services.
- Do not browse to untrusted websites.
- Consider disabling the TIFF and/or PNG attachment distillers until patches can be applied.

REFERENCES:**Research in Motion:**

<http://blackberry.com/btsc/KB27244>

Security Focus:

<http://www.securityfocus.com/bid/49098>

Secunia:

<http://secunia.com/advisories/45580>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0192>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1167>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1205>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2595>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3087>