

*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:**

10/14/2010

**SUBJECT:**

Vulnerability in BlackBerry Attachment Service Could Allow Remote Code Execution

**OVERVIEW:**

A vulnerability has been discovered in the BlackBerry Attachment Service. The BlackBerry Attachment Service is a component of BlackBerry Enterprise Server and BlackBerry Professional Software that is used to process email attachments. These vulnerabilities affect the Blackberry Enterprise Server; not the Blackberry mobile device. Successful exploitation may result in an attacker gaining complete control of the Blackberry Enterprise Server. Depending on the privileges associated with the service, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

**SYSTEMS AFFECTED:**

BlackBerry Enterprise Server software version 5.02 and earlier  
BlackBerry Professional Software 4.1 Service Pack 4 (4.1.4)

**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:**

A vulnerability has been discovered in the BlackBerry Attachment Service on the BlackBerry Enterprise Server. This vulnerability can be leveraged when the Attachment Service's PDF distiller attempts to process a specially crafted PDF file. The PDF distiller is a component of the Attachment Service that processes PDF files and converts them to a format that is easily rendered on a BlackBerry mobile device. Successful exploitation may result in an attacker gaining complete control of the affected system. Depending on the privileges associated with the service, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition. There are no known exploits for this vulnerability at this time.

**RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Research in Motion to vulnerable systems immediately after appropriate testing.
- Do not open email attachments from unknown or un-trusted sources.
- Consider disabling the PDF attachment distiller until patches can be applied.

**REFERENCES:**

**Research in Motion:**

<http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB24547>

**Security Focus:**

<http://www.securityfocus.com/bid/44056>