

# State of Alaska State Security Office



## State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

January 11, 2011

*The following cyber advisory was issued by the State of Alaska and was 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.*

**ADVISORY NUMBER:**

SA2011-003

**DATE(S) ISSUED:**

01/11/2011

**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. This vulnerability affects the BlackBerry Enterprise Server; not the BlackBerry mobile device. Successful exploitation could result in an attacker gaining the same privileges as the BlackBerry Attachment Service and possibly the highest privilege level. 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 exploitation could result in denial-of-service conditions.

**SYSTEMS AFFECTED:**

- BlackBerry Enterprise Server Express version 5.0.1 and 5.0.2 for Microsoft Exchange
- BlackBerry Enterprise Server Express version 5.0.2 for IBM Lotus Domino
- BlackBerry Enterprise Server versions 4.1.3 through 5.0.2 for Microsoft Exchange and IBM Lotus Domino
- BlackBerry Enterprise Server versions 4.1.3 through 5.0.1 for Novell GroupWise
- BlackBerry Professional Software version 4.1.4 for Microsoft Exchange and 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:**

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. To exploit this vulnerability, a BlackBerry smartphone user would open a specially crafted PDF file. This could occur by opening an email attachment or clicking on a link on a website. Successful exploitation could result in an attacker gaining the same privileges as the BlackBerry Attachment Service and even as high as SYSTEM level. 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 exploitation could result in denial-of-service conditions.

**RECOMMENDATIONS:**

We recommend the following actions 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.
- Do not browse to un-trusted websites.
- 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=KB25382>

**Security Focus:**

<http://www.securityfocus.com/bid/45753>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2604>