



State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory

November 4, 2009

*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:**

SA2009-062

**DATE(S) ISSUED:**

11/4/2009

**SUBJECT:**

BlackBerry ActiveX Remote Code Execution Vulnerability

**OVERVIEW:**

A vulnerability has been discovered in the BlackBerry Desktop Manager that could allow remote code execution. Research In Motion BlackBerry Desktop Manager is used to synchronize smart phones and desktop computers. Exploitation may occur if a user visits a specifically crafted web page which takes advantage of these vulnerabilities. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, 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:**

- Research In Motion Blackberry Desktop Manager 4.2.2
- Research In Motion Blackberry Desktop Manager 4.7
- Research In Motion Blackberry Desktop Manager 5.0

**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: High

### DESCRIPTION:

A vulnerability has been discovered in Research In Motion BlackBerry Desktop Manager that could allow an attacker to take complete control of an affected system. This issue occurs in the Lotus Notes Intellisync ActiveX control provided by 'Inresobject.dll'. The control is identified by the following CLSID:

{158CD9E8-E195-4E82-9A78-0CF6B86B3629}

Exploitation may occur if a user visits a specifically crafted web page which takes advantage of these vulnerabilities. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, 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. The BlackBerry Desktop Manager does not need to be running for a malicious user to exploit this vulnerability.

Please note that the Lotus Notes Intellisync ActiveX control provided by the 'Inresobject.dll' may be present regardless of whether you have Lotus Notes deployed.

### RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by BlackBerry to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Set the kill bit on the Class Identifier (CLSID) {158CD9E8-E195-4E82-9A78-0CF6B86B3629}; further instructions on how to set the kill bit can be found at the following location (<http://support.microsoft.com/kb/240797>).

### REFERENCES:

#### BlackBerry:

<http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB19701>

#### Microsoft:

<http://support.microsoft.com/kb/240797>

#### Security Focus:

<http://www.securityfocus.com/bid/36903>

#### CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0306>