

# [NEWS] BlackBerry Attachment Service Buffer Overflow (.doc file)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00042.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 13 Feb 2006 19:22:11 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

BlackBerry Attachment Service Buffer Overflow (.doc file)

---

## SUMMARY

" <<http://www.blackberry.com/products/software/index.shtml>> BlackBerry Enterprise Server software sits behind your organization's firewall and is designed to tightly integrate with existing enterprise systems, securely extending wireless communications and corporate data to mobile users."

A specially crafted Microsoft Word (.doc) file opened on a BlackBerry device could potentially allow code execution.

## DETAILS

### Vulnerable Systems:

- \* BlackBerry Enterprise Server for IBM Lotus Domino version 2.2 and above
- \* BlackBerry Enterprise Server for Microsoft Exchange version 3.6 and above
- \* BlackBerry Enterprise Server for Novell GroupWise version 4.0 and above

A corrupt Microsoft Word (.doc) file opened on a BlackBerry wireless

## [NEWS] BlackBerry Attachment Service Buffer Overflow (.doc file)

device could potentially provide a means to execute arbitrary code on the BlackBerry Attachment Service component of the BlackBerry Enterprise Server.

### Workaround:

An administrator can exclude Microsoft Word files from being processed by the Attachment Service in the BlackBerry Enterprise Server, or disable the Attachment Service completely.

To exclude Microsoft Word files from being processed by the Attachment Service

1. On the desktop, click Start > Programs > BlackBerry Enterprise Server

### BlackBerry Enterprise Server Configuration.

2. Click the Attachment Server tab.

3. In the Format Extensions field, delete the .doc extension.

Note: Format Extensions is an editable field that lists all the extensions that the Attachment Service will open. A colon is used as a delimiter.

4. Click Apply, then click OK.

Even though the .doc extension has been removed from the list of supported file types, the Attachment Service may automatically detect a .doc file with a renamed extension and attempt to process the file. Administrators may need to disable the Attachment Service.

To disable the Attachment Service

1. In Microsoft Windows Administrative Tools, double-click Services.
2. Right-click BlackBerry Attachment Service, then click Stop.
3. Close the Services window.

### Vendor Status:

Depending on your environment and the BlackBerry Enterprise Server version, install the appropriate software upgrades.

### Microsoft Exchange:

For BlackBerry Enterprise Server 3.6, install Service Pack 7.

For BlackBerry Enterprise Server 4.0, install Service Pack 3, then install version 4.0 Service Pack 3 Hotfix 3.

### IBM Lotus Domino:

For BlackBerry Enterprise Server 2.2, a resolution for this issue has been developed and is currently undergoing testing. A software upgrade will be made available as soon as testing is complete.

For BlackBerry Enterprise Server 4.0, install Service Pack 3, then install version 4.0 Service Pack 3 Hotfix 4.

### Novell GroupWise:

Install BlackBerry Enterprise Server 4.0 Service Pack 3, then install version 4.0 Service Pack 3 Hotfix 1.

To obtain the BlackBerry Enterprise Server software, go to the <http://www.blackberry.com/support/downloads/index.shtml> > BlackBerry

[NEWS] BlackBerry Attachment Service Buffer Overflow (.doc file)

Software Download Information web site.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:lukew@xxxxxxxxxx>> lukew.

The original article can be found at:

[http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8021/8149/8052/Support – Corrupt Wo](http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8021/8149/8052/Support%20-%20Corrupt%20Words)

[http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8021/8149/8052/Support – Corrupt Wor](http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8021/8149/8052/Support%20-%20Corrupt%20Words)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.