



CVE-2006-0761

Published on: 02/17/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:07 PM UTC

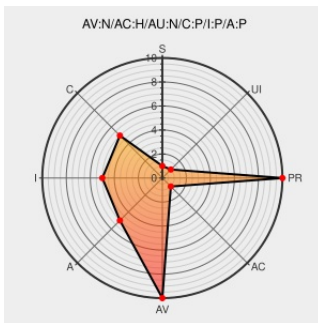
CVE-2006-0761

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Blackberry Enterprise Server](#) from [Rim](#) contain the following vulnerability:

Buffer overflow in BlackBerry Attachment Service in Research in Motion (RIM) BlackBerry Enterprise Server 2.2 and 4.0 before SP3 Hotfix 4 for IBM Lotus Domino, 3.6 before SP7 and 5.0 before SP3 Hotfix 3 for Microsoft Exchangem, and 4.0 for Novell GroupWise before SP3 Hotfix 1 might allow user-assisted remote attackers to execute

arbitrary code on the server via a crafted Microsoft Word document that is opened on a wireless device.

CVE-2006-0761 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.1 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force
Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF blackberry-attachment-word-bo\(24629\)](#)

Support -
Corrupt Word
file may cause
buffer overflow
in the
BlackBerry
Attachment
Service

[web.archive.org](https://web.archive.org/text/html)
[text/html](#)
Inactive Link **Not Archived**

CONFIRM
www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8021/8149/8052/Support_Corrupt_Word_file_may_cause_buffer_overflow_in_the_BlackBerry_Attachment_Service.htnodeid=1181753&vernum=2

SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060210 Corrupt Word file may cause buffer overflow in the Blackberry Attachment Service
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-0530
BlackBerry Enterprise Server Malformed Word Attachment Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 16590

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.



There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rim	Blackberry Enterprise Server	2.2	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp2	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp2a	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp3a	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp4	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp4_hotfix2	All	All	All
Application	Rim	Blackberry Enterprise Server	3.6	All	exchange	All
Application	Rim	Blackberry Enterprise Server	3.6.1	All	exchange	All
Application	Rim	Blackberry Enterprise Server	3.6_sp1a	All	exchange	All
Application	Rim	Blackberry Enterprise Server	3.6_sp4_hotfix2	All	exchange	All
Application	Rim	Blackberry Enterprise Server	4.0	All	domino	All
Application	Rim	Blackberry Enterprise Server	4.0	All	novell_groupwise	All
Application	Rim	Blackberry Enterprise Server	4.0_sp1	All	domino	All
Application	Rim	Blackberry Enterprise Server	4.0_sp1	All	novell_groupwise	All
Application	Rim	Blackberry Enterprise Server	4.0_sp2	All	domino	All
Application	Rim	Blackberry Enterprise Server	4.0_sp2	All	novell_groupwise	All
Application	Rim	Blackberry Enterprise Server	4.0_sp3	All	domino	All

Application	Rim	Blackberry Enterprise Server	4.0_sp3	All	novell_groupwise	All
Application	Rim	Blackberry Enterprise Server	2.2	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp2	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp2a	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp3a	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp4	All	All	All
Application	Rim	Blackberry Enterprise Server	2.2_sp4_hotfix2	All	All	All
Application	Rim	Blackberry Enterprise Server	3.6	All	exchange	All
Application	Rim	Blackberry Enterprise Server	3.6.1	All	exchange	All
Application	Rim	Blackberry Enterprise Server	3.6_sp1a	All	exchange	All
Application	Rim	Blackberry Enterprise Server	3.6_sp4_hotfix2	All	exchange	All
Application	Rim	Blackberry Enterprise Server	4.0	All	domino	All
Application	Rim	Blackberry Enterprise Server	4.0	All	novell_groupwise	All
Application	Rim	Blackberry Enterprise Server	4.0_sp1	All	domino	All
Application	Rim	Blackberry Enterprise Server	4.0_sp1	All	novell_groupwise	All
Application	Rim	Blackberry Enterprise Server	4.0_sp2	All	domino	All
Application	Rim	Blackberry Enterprise Server	4.0_sp2	All	novell_groupwise	All
Application	Rim	Blackberry Enterprise Server	4.0_sp3	All	domino	All
Application	Rim	Blackberry Enterprise Server	4.0_sp3	All	novell_groupwise	All
cpe:2.3:a:r:blackberry_enterprise_server:2.2:*:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:2.2_sp2:*:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:2.2_sp2a:*:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:2.2_sp3a:*:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:2.2_sp4:*:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:2.2_sp4_hotfix2:*:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:3.6:*:exchange:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:3.6.1:*:exchange:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:3.6_sp1a:*:exchange:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:3.6_sp4_hotfix2:*:exchange:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:4.0:*:domino:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:4.0:*:novell_groupwise:*:*:*:*:						
cpe:2.3:a:r:blackberry_enterprise_server:4.0_sp1:*:domino:*:*:*:*:						

cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp1*:novell_groupwise:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp2*:domino:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp2*:novell_groupwise:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp3*:domino:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp3*:novell_groupwise:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:2.2*:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:2.2_sp2:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:2.2_sp2a:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:2.2_sp3a:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:2.2_sp4:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:2.2_sp4_hotfix2:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:3.6*:exchange:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:3.6.1*:exchange:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:3.6_sp1a*:exchange:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:3.6_sp4_hotfix2*:exchange:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0*:domino:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0*:novell_groupwise:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp1*:domino:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp1*:novell_groupwise:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp2*:domino:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp2*:novell_groupwise:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp3*:domino:*****:
cpe:2.3:a:rim:blackberry_enterprise_server:4.0_sp3*:novell_groupwise:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)