



CVE-2004-1264

Published on: 12/22/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1264

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Chbg](#) from [Chbg](#) contain the following vulnerability:

Buffer overflow in the simplify_path function in config.c for ChBg 1.5 allows remote attackers to execute arbitrary code via a crafted chbg scenario file.

CVE-2004-1264 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Advisories - Mandriva Linux

[www.mandriva.com](#)
[text/html](#)

[MANDRAKE MDKSA-2005:027](#)

IBM X-Force Exchange

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

[XF chbg-simplifypath-bo\(18595\)](#)

Debian -- Security Information -- DSA-644-1 chbg

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-644](#)

404 Not Found

[Exploit](#)
[Vendor Advisory](#)
[tigger.uic.edu](#)
[text/plain](#)
[Inactive Link](#) [Not Archived](#)

[MISC tigger.uic.edu/~jlongs2/holes/chbg.txt](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

By selecting these links, you may be leaving CVEreport's website. We have provided these links to other resources 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	Chbg	Chbg	1.5	All	All	All
Application	Chbg	Chbg	1.5	All	All	All
cpe:2.3:a:chbg:chbg:1.5:*****:						
cpe:2.3:a:chbg:chbg:1.5:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →