



CVE-2004-1309

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

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

CVE-2004-1309

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

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

Heap-based buffer overflow in the demux_open_bmp function in demux_bmp.c for Unix MPlayer 1.0pre5 allows remote attackers to execute arbitrary code via a bitmap (BMP) file containing a large biClrUsed field.

CVE-2004-1309 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

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

[MANDRAKE MDKSA-2004:157](#)

iDEFENSE

[Vendor Advisory](#)
www.idefense.com
[text/html](#)

[IDEFENSE 20041216 MPlayer Bitmap Parsing Remote Heap Overflow Vulnerability](#)

403 Forbidden

www1.mplayerhq.hu
[text/plain](#)
Inactive Link **Not Archived**

[CONFIRM www1.mplayerhq.hu/MPlayer/releases/ChangeLog](#)

IBM X-Force
Exchange

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

[XF mplayer-bitmap-bo\(18527\)](#)

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,

are more appropriate for your purposes. CVEreport does not necessarily endorse the views expressed, or content, that are linked presented on these sites. 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	Mplayer	Unix Mplayer	1.0_pre5	All	All	All
Application	Mplayer	Unix Mplayer	1.0_pre5	All	All	All
cpe:2.3:a:mplayer:unix_mplayer:1.0_pre5:*****::						
cpe:2.3:a:mplayer:unix_mplayer:1.0_pre5:*****::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)