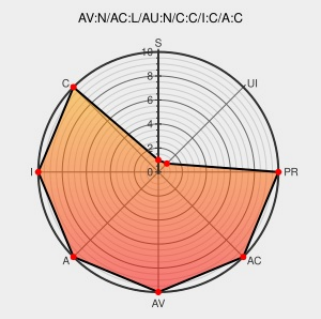
# CVE-2004-1309

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 cve@mitre.org to track the vulnerability

### CVSS2 Score: 10 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Advisories - Mandriva | www.mandriva.com<br>text/html | MANDRAKE MDKSA-2004:157 |
| iDEFENSE | Vendor Advisory<br>www.idefense.com<br>text/html | IDEFENSE 20041216 MPlayer Bitmap Parsing Remote Heap Overflow Vulnerability |
| 403 Forbidden | www1.mplayerhq.hu<br>text/plain<br>Inactive Link Not Archived | CONFIRM www1.mplayerhq.hu/MPlayer/releases/ChangeLog |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com<br>text/html | XF mplayer-bitmap-bo(18527) |

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→