

Henson Scap

Details of Vulnerabilities as of 2013-12-11

See next page

# Of Vuls	CVE-ID	Summary	Vulnerable Software
1	CVE-2013-0845	libavcodec/alsdec.c in FFmpeg before 1.0.4 allows remote attackers to have an unspecified impact via a crafted block length, which triggers an out-of-bounds write.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:1.0.2", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:1.0.1", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
2	CVE-2013-0844	Off-by-one error in the adpcm_decode_frame function in libavcodec/adpcm.c in FFmpeg before 1.0.4 allows remote attackers to have an unspecified impact via crafted DK4 data, which triggers an out-of-bounds array access.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:1.0.2", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:1.0.1", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
3	CVE-2013-0858	The atrac3_decode_init function in libavcodec/atrac3.c in FFmpeg before 1.0.4 allows remote attackers to have an unspecified impact via ATRAC3 data with the joint stereo coding mode set and fewer than two channels.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:1.0.2", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:1.0.1", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
4	CVE-2013-0854	The mjpeg_decode_scan_progressive_ac function in libavcodec/mjpegdec.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted MJPEG data.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
5	CVE-2013-0847	The ff_id3v2_parse function in libavformat/id3v2.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via ID3v2 header data, which triggers an out-of-bounds array access.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
6	CVE-2013-0852	The parse_picture_segment function in libavcodec/pgssubdec.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted RLE data, which triggers an out-of-bounds array access.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
7	CVE-2013-0857	The decode_frame_ilbm function in libavcodec/iff.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a crafted height value in IFF PBM/ILBM bitmap data.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
8	CVE-2013-0850	The decode_slice_header function in libavcodec/h264.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted H.264 data, which triggers an out-of-bounds array access.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
9	CVE-2013-0846	Array index error in the qdm2_decode_super_block function in libavcodec/qdm2.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted QDM2 data, which triggers an out-of-bounds array access.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
10	CVE-2013-0851	The decode_frame function in libavcodec/eamad.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted Electronic Arts Madcow video data, which triggers an out-of-bounds array access.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
11	CVE-2013-0859	The add_doubles_metadata function in libavcodec/tiff.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a negative or zero count value in a TIFF image, which triggers an out-of-bounds array access.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
12	CVE-2013-0853	The wavpack_decode_frame function in libavcodec/wavpack.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted WavPack data, which triggers an out-of-bounds array access, possibly due to an off-by-one error.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
13	CVE-2013-0856	The lpc_prediction function in libavcodec/alac.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted Apple Lossless Audio Codec (ALAC) data, related to a large nb_samples value.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
14	CVE-2013-0849	The roq_decode_init function in libavcodec/roqvideodec.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a crafted (1) width or (2) height dimension that is not a multiple of sixteen in id RoQ video data.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
15	CVE-2013-0848	The decode_init function in libavcodec/huffyuv.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a crafted width in huffyuv data with the predictor set to median and the colorspace set to YUV422P, which triggers an out-of-bounds array access.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
16	CVE-2013-0855	Integer overflow in the alac_decode_close function in libavcodec/alac.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a large number of samples per frame in Apple Lossless Audio Codec (ALAC) data, which triggers an out-of-bounds array access.	["cpe:/a:ffmpeg:ffmpeg:0.4.0", "cpe:/a:ffmpeg:ffmpeg:0.4.4", "cpe:/a:ffmpeg:ffmpeg:0.4.3", "cpe:/a:ffmpeg:ffmpeg:0.4.2", "cpe:/a:ffmpeg:ffmpeg:0.4.7", "cpe:/a:ffmpeg:ffmpeg:0.4.6", "cpe:/a:ffmpeg:ffmpeg:0.4.9:pre1", "cpe:/a:ffmpeg:ffmpeg:0.4.5", "cpe:/a:ffmpeg:ffmpeg:0.5", "cpe:/a:ffmpeg:ffmpeg:0.3", "cpe:/a:ffmpeg:ffmpeg:0.6", "cpe:/a:ffmpeg:ffmpeg:0.7.5", "cpe:/a:ffmpeg:ffmpeg:0.10", "cpe:/a:ffmpeg:ffmpeg:0.11", "cpe:/a:ffmpeg:ffmpeg:0.8.6", "cpe:/a:ffmpeg:ffmpeg:0.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5", "cpe:/a:ffmpeg:ffmpeg:0.9", "cpe:/a:ffmpeg:ffmpeg:0.8.8", "cpe:/a:ffmpeg:ffmpeg:0.8.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.4", "cpe:/a:ffmpeg:ffmpeg:0.7.8", "cpe:/a:ffmpeg:ffmpeg:0.7.9", "cpe:/a:ffmpeg:ffmpeg:0.7.6", "cpe:/a:ffmpeg:ffmpeg:0.7.7", "cpe:/a:ffmpeg:ffmpeg:0.8.5.3", "cpe:/a:ffmpeg:ffmpeg:0.7.12", "cpe:/a:ffmpeg:ffmpeg:0.4.8", "cpe:/a:ffmpeg:ffmpeg:0.7.11", "cpe:/a:ffmpeg:ffmpeg:0.5.2", "cpe:/a:ffmpeg:ffmpeg:0.10.4", "cpe:/a:ffmpeg:ffmpeg:0.5.3", "cpe:/a:ffmpeg:ffmpeg:0.8.0", "cpe:/a:ffmpeg:ffmpeg:0.5.1", "cpe:/a:ffmpeg:ffmpeg:0.10.3", "cpe:/a:ffmpeg:ffmpeg:0.8.2", "cpe:/a:ffmpeg:ffmpeg:0.8.1", "cpe:/a:ffmpeg:ffmpeg:0.5.4", "cpe:/a:ffmpeg:ffmpeg:0.8.11", "cpe:/a:ffmpeg:ffmpeg:0.8.10", "cpe:/a:ffmpeg:ffmpeg:0.6.1", "cpe:/a:ffmpeg:ffmpeg:0.7.3", "cpe:/a:ffmpeg:ffmpeg:0.6.2", "cpe:/a:ffmpeg:ffmpeg:0.7.2", "cpe:/a:ffmpeg:ffmpeg:1.0", "cpe:/a:ffmpeg:ffmpeg:0.5.4.6", "cpe:/a:ffmpeg:ffmpeg:0.7.4", "cpe:/a:ffmpeg:ffmpeg:0.5.4.5", "cpe:/a:ffmpeg:ffmpeg:0.6.3", "cpe:/a:ffmpeg:ffmpeg:0.7.1", "cpe:/a:ffmpeg:ffmpeg:0.3.2", "cpe:/a:ffmpeg:ffmpeg:0.3.3", "cpe:/a:ffmpeg:ffmpeg:0.3.4", "cpe:/a:ffmpeg:ffmpeg:0.9.1", "cpe:/a:ffmpeg:ffmpeg:0.3.1"]
17	CVE-2013-7021	The filter_frame function in libavfilter/vf_fps.c in FFmpeg before 2.1 does not properly ensure the availability of FIFO content, which allows remote attackers to cause a denial of service (double free) or possibly have unspecified other impact via crafted data.	No software given

# Of Vuls	CVE-ID	Summary	Vulnerable Software
18	CVE-2013-7014	Integer signedness error in the add_bytes_l2_c function in libavcodec/pngdsp.c in FFmpeg before 2.1 allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted PNG data.	No software given
19	CVE-2013-7022	The g2m_init_buffers function in libavcodec/g2meet.c in FFmpeg before 2.1 does not properly allocate memory for tiles, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Go2Webinar data.	No software given
20	CVE-2013-7019	The get_cox function in libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not properly validate the reduction factor, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	No software given
21	CVE-2013-7016	The get_siz function in libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not ensure the expected sample separation, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	No software given

# Of Vuls	CVE-ID	Summary	Vulnerable Software
22	CVE-2013-7011	The read_header function in libavcodec/ffv1dec.c in FFmpeg before 2.1 does not prevent changes to global parameters, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted FFV1 data.	No software given
23	CVE-2013-7008	The decode_slice_header function in libavcodec/h264.c in FFmpeg before 2.1 incorrectly relies on a certain droppable field, which allows remote attackers to cause a denial of service (deadlock) or possibly have unspecified other impact via crafted H.264 data.	No software given
24	CVE-2013-7024	The jpeg2000_decode_tile function in libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not consider the component number in certain calculations, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	No software given
25	CVE-2013-7023	The ff_combine_frame function in libavcodec/parser.c in FFmpeg before 2.1 does not properly handle certain memory-allocation errors, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted data.	No software given

# Of Vuls	CVE-ID	Summary	Vulnerable Software
26	CVE-2013-7018	libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not ensure the use of valid code-block dimension values, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	No software given
27	CVE-2013-7013	The g2m_init_buffers function in libavcodec/g2meet.c in FFmpeg before 2.1 uses an incorrect ordering of arithmetic operations, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Go2Webinar data.	No software given
28	CVE-2013-7009	The rpza_decode_stream function in libavcodec/rpza.c in FFmpeg before 2.1 does not properly maintain a pointer to pixel data, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Apple RPZA data.	No software given
29	CVE-2013-7015	The flashsv_decode_frame function in libavcodec/flashsv.c in FFmpeg before 2.1 does not properly validate a certain height value, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Flash Screen Video data.	No software given

# Of Vuls	CVE-ID	Summary	Vulnerable Software
30	CVE-2013-7012	The get_siz function in libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not prevent attempts to use non-zero image offsets, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	No software given
31	CVE-2013-7017	libavcodec/jpeg2000.c in FFmpeg before 2.1 allows remote attackers to cause a denial of service (invalid pointer dereference) or possibly have unspecified other impact via crafted JPEG2000 data.	No software given
32	CVE-2013-7010	Multiple integer signedness errors in libavcodec/dsputil.c in FFmpeg before 2.1 allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted data.	No software given
33	CVE-2013-7020	The read_header function in libavcodec/ffv1dec.c in FFmpeg before 2.1 does not properly enforce certain bit-count and colorspace constraints, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted FFV1 data.	No software given
34	CVE-2011-3935	The codec_get_buffer function in ffmpeg.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via vectors related to a crafted image size.	No software given

# Of Vuls	CVE-ID	Summary	Vulnerable Software
35	CVE-2011-3944	The smacker_decode_header_tree function in libavcodec/smacker.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via crafted Smacker data.	No software given
36	CVE-2011-3949	The dirac_unpack_idwt_params function in libavcodec/diracdec.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via crafted Dirac data.	No software given
37	CVE-2011-3950	The dirac_decode_data_unit function in libavcodec/diracdec.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via a crafted value in the reference pictures number.	No software given
38	CVE-2011-3934	Double free vulnerability in the vp3_update_thread_context function in libavcodec/vp3.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via crafted vp3 data.	No software given
39	CVE-2011-3941	The decode_mb function in libavcodec/error_resilience.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via vectors related to an uninitialized block index, which triggers an out-of-bound write.	No software given
40	CVE-2011-3946	The ff_h264_decode_sei function in libavcodec/h264_sei.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via crafted Supplemental enhancement information (SEI) data, which triggers an infinite loop.	No software given

# Of Vuls	CVE-ID	Summary	Vulnerable Software
41	CVE-2011-4351	Buffer overflow in FFmpeg before 0.5.6, 0.6.x before 0.6.4, 0.7.x before 0.7.8, and 0.8.x before 0.8.8 allows remote attackers to execute arbitrary code via unspecified vectors.	No software given