



Published on: 09/28/2011 12:00:00 AM UTC

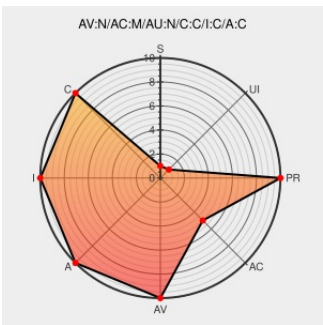
Last Modified on: 03/23/2021 11:23:14 PM UTC

# CVE-2011-3504

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of `Ffmpeg` from `Ffmpeg` contain the following vulnerability:

The Matroska format decoder in FFmpeg before 0.8.3 does not properly allocate memory, which allows remote attackers to execute arbitrary code via a crafted file.

CVE-2011-3504 has been assigned by  [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: 9.3 - HIGH

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

## CVE References

| Description                                   | Tags                                                                                        | Link                                                                                                                                                                                                              |
|-----------------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | <a href="#">www.ffmpeg.org</a><br><a href="#">text/plain</a>                                |  MISC<br><a href="https://www.ffmpeg.org/releases/ffmpeg-0.8.4.changelog">www.ffmpeg.org/releases/ffmpeg-0.8.4.changelog</a> |
| No Description Provided                       | <a href="#">www.osvdb.org</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  OSVDB 75621                                                                                                                 |
| FFmpeg Multiple Vulnerabilities - Secunia.com | <a href="#">web.archive.org</a><br><a href="#">text/html</a>                                |  SECUNIA 45532                                                                                                               |
| USN-1333-1: Libav vulnerabilities   Ubuntu    | <a href="#">ubuntu.com</a><br><a href="#">text/html</a>                                     |  UBUNTU USN-1333-1                                                                                                           |
| USN-1320-1: FFmpeg vulnerabilities   Ubuntu   | <a href="#">ubuntu.com</a><br><a href="#">text/html</a>                                     |  UBUNTU USN-1320-1                                                                                                           |

|                                                                                                                                         |                                                                                          |                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Support / Security / Advisories // MDVSA-2012:075   Mandriva                                                                            | <a href="http://www.mandriva.com/text/html">www.mandriva.com<br/>text/html</a>           |  <b>MANDRIVA MDVSA-2012:075</b>                                                                                                                 |
| Support / Security / Advisories // MDVSA-2012:074   Mandriva                                                                            | <a href="http://www.mandriva.com/text/html">www.mandriva.com<br/>text/html</a>           |  <b>MANDRIVA MDVSA-2012:074</b>                                                                                                                |
| Support / Security / Advisories // MDVSA-2012:076   Mandriva                                                                            | <a href="http://www.mandriva.com/text/html">www.mandriva.com<br/>text/html</a>           |  <b>MANDRIVA MDVSA-2012:076</b>                                                                                                                |
| Microsoft Vulnerability Research Advisory MSVR11-011: Vulnerability in FFmpeg Matroska Format Decoder Could Allow Remote Code Execution | <a href="http://technet.microsoft.com/text/html">technet.microsoft.com<br/>text/html</a> |  <b>MISC</b><br><a href="http://technet.microsoft.com/en-us/security/msvr/msvr11-011">technet.microsoft.com/en-us/security/msvr/msvr11-011</a> |
|                                                                                                                                         | <a href="http://www.ffmpeg.org/text/plain">www.ffmpeg.org<br/>text/plain</a>             |  <b>MISC</b><br><a href="http://www.ffmpeg.org/releases/ffmpeg-0.7.5.changelog">www.ffmpeg.org/releases/ffmpeg-0.7.5.changelog</a>             |

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](mailto: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 | Ffmpeg | Ffmpeg  | 0.3     | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.3.1   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.3.2   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.3.3   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.3.4   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.0   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.2   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.3   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.4   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.5   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.6   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.7   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.8   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.9   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.4.9   | pre1   | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.5     | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.5.1   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.5.2   | All    | All     | All      |
| Application | Ffmpeg | Ffmpeg  | 0.5.3   | All    | All     | All      |

|                                      |        |        |       |      |     |     |
|--------------------------------------|--------|--------|-------|------|-----|-----|
| Application                          | Ffmpeg | Ffmpeg | 0.5.4 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.6   | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.6.1 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.6.2 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | All   | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.3   | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.3.1 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.3.2 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.3.3 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.3.4 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.0 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.2 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.3 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.4 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.5 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.6 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.7 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.8 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.9 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.4.9 | pre1 | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.5   | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.5.1 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.5.2 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.5.3 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.5.4 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.6   | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.6.1 | All  | All | All |
| Application                          | Ffmpeg | Ffmpeg | 0.6.2 | All  | All | All |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3:*****:   |        |        |       |      |     |     |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3.1:*****: |        |        |       |      |     |     |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3.2:*****: |        |        |       |      |     |     |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3.3:*****: |        |        |       |      |     |     |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3.4:*****: |        |        |       |      |     |     |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.0:*****: |        |        |       |      |     |     |

|                                               |
|-----------------------------------------------|
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.2:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.3:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.4:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.5:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.6:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.7:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.8:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.9:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.9:pre1:*:*:*:*:*: |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5:*:*:*:*:*:        |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5.1:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5.2:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5.3:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5.4:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.6:*:*:*:*:*:        |
| cpe:2.3:a:ffmpeg:ffmpeg:0.6.1:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.6.2:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:*:*:*:*:*:            |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3:*:*:*:*:*:        |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3.1:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3.2:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3.3:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.3.4:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.0:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.2:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.3:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.4:*:*:*:*:*:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.5:*:*:*:*:*:      |

|                                           |
|-------------------------------------------|
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.6:*****:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.7:*****:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.8:*****:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.9:*****:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.4.9:pre1:*****: |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5:*****:        |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5.1:*****:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5.2:*****:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5.3:*****:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.5.4:*****:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.6:*****:        |
| cpe:2.3:a:ffmpeg:ffmpeg:0.6.1:*****:      |
| cpe:2.3:a:ffmpeg:ffmpeg:0.6.2:*****:      |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)