



# CVE-2016-7122

Published on: 12/23/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:06 PM UTC

## CVE-2016-7122

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

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

The `avi_read_nikon` function in `libavformat/avidec.c` in `FFmpeg` before 3.1.4 is vulnerable to infinite loop when it decodes an AVI file that has a crafted 'nctg' structure.

CVE-2016-7122 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                                                                        | Tags                                                                                                                                  | Link                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| oss-security - ffmpeg before 3.1.4 [CVE-2016-7562] [CVE-2016-7122] [CVE-2016-7450] [CVE-2016-7502] [CVE-2016-7555] [CVE-2016-7785] [CVE-2016-7905] | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a><br><a href="#">www.openwall.com</a><br><a href="#">text/html</a> | <a href="#">MLIST [oss-security] 20161008 ffmpeg before 3.1.4 [CVE-2016-7562] [CVE-2016-7122] [CVE-2016-7450] [CVE-2016-7502] [CVE-2016-7555] [CVE-2016-7785] [CVE-2016-7905]</a> |

FFmpeg: Multiple vulnerabilities (GLSA 201701-71) —  
Gentoo security

[security.gentoo.org](#)  
[text/html](#)

 GENTOO GLSA-201701-71

FFmpeg 'libavformat/avidec.c' Denial of Service  
Vulnerability

[cve.report \(archive\)](#)  
[text/html](#)

 BID 94839

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).

Related QID Numbers

710513 Gentoo Linux FFmpeg Multiple Vulnerabilities (GLSA 201701-71)

Known Affected Configurations (CPE V2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Ffmpeg | Ffmpeg  | All     | All    | All     | All      |

cpe:2.3:a:ffmpeg:ffmpeg:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →