

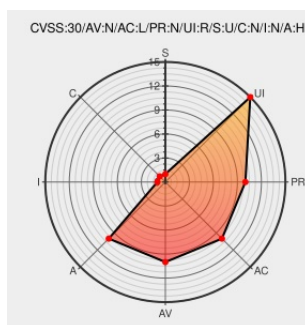


CVE-2018-5816

Published on: 12/07/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

CVE-2018-5816

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

An integer overflow error within the "identify()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.12 can be exploited to trigger a division by zero via specially crafted NOKIARAW file (Note: This vulnerability is caused due to an incomplete fix of CVE-2018-5804).

CVE-2018-5816 has been assigned by PSIRT-CNA@flexerasoftware.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **7.1 - HIGH**

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

CVE References

Description	Tags	Link
LibRaw/Changelog.txt at master · LibRaw/LibRaw · GitHub	Third Party Advisory github.com	MISC github.com/LibRaw/LibRaw/blob/master/Changelog.txt

Patch
Third Party Advisory
github.com
text/html

Permissions Required

Third Party Advisory

secuniaresearch.flexerasoftware.com

text/html



Third Party Advisory
secuniaresearch.flexerasoftware.com
text/html



Third Party Advisory
usn.ubuntu.com
text/html

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Application	Libraw	Libraw	All	All	All	All
Application	Libraw	Libraw	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:its:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:its:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:its:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:its:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:its:*:*:						

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:
cpe:2.3:a:libraw:libraw:*:*:*:*:*:
cpe:2.3:a:libraw:libraw:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID→](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)