



# CVE-2018-5801

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-5801
<b>State</b>	PUBLIC
<b>Assigner</b>	PSIRT-CNA@flexerasoftware.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-07 22:29:00 UTC
<b>Updated</b>	2019-03-29 14:21:00 UTC
<b>Description</b>	An error within the "LibRaw::unpack()" function (src/libraw_cxx.cpp) in LibRaw versions prior to 0.18.7 can be exploited to tr

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Libraw</a>	<a href="#">Libraw</a>	All	All	All	All
Application	<a href="#">Libraw</a>	<a href="#">Libraw</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

References			
Reference	Source	Link	Tags
SA79000 advisory fix · LibRaw/LibRaw@0df5490 · GitHub	MISC	<a href="#">github.com</a>	Patch
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>	Third Party Advisory
LibRaw/Changelog.txt at master · LibRaw/LibRaw · GitHub	MISC	<a href="#">github.com</a>	Release Notes
[SECURITY] [DLA 1734-1] libraw security update	MLIST	<a href="#">lists.debian.org</a>	Mailing List, Third Party
End of Support for the Secunia Community Site - Community	SECUNIA	<a href="#">secuniaresearch.flexerasoftware.com</a>	Third Party Advisory
USN-3615-1: LibRaw vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubuntu.com</a>	Third Party Advisory
Secunia Research Advisories   Flexera	MISC	<a href="#">secuniaresearch.flexerasoftware.com</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [179045](#) Debian Security Update for libraw (DLA 2903-1)
- [752153](#) SUSE Enterprise Linux Security Update for ddraw (SUSE-SU-2022:1749-1)

© CVE.report 2026 |

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](#)**