libTIFF: Multiple vulnerabilities — GLSA 201709-27

Multiple vulnerabilities have been found in LibTIFF, the worst of which could result in the execution of arbitrary code.

Affected packages

Package	**media-libs/tiff** on all architectures
Affected versions	< **4.0.8**
Unaffected versions	>= **4.0.8**

Background

The TIFF library contains encoding and decoding routines for the Tag Image File Format. It is called by numerous programs, including GNOME and KDE applications, to interpret TIFF images.

Description

Multiple vulnerabilities have been discovered in LibTIFF. Please review the referenced CVE identifiers for details.

Impact

A remote attacker, by enticing the user to process a specially crafted TIFF file, could possibly execute arbitrary code with the privileges of the process, cause a Denial of Service condition, obtain sensitive information, or have other unspecified impacts.

Workaround

There is no known workaround at this time.

Resolution

All LibTIFF users should upgrade to the latest version:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=media-libs/tiff-4.0.8"
```

Packages which depend on this library may need to be recompiled. Tools such as revdep-rebuild may assist in identifying some of these packages.

References

- CVE-2016-10267
- CVE-2016-10268
- CVE-2017-5225
- CVE-2017-5563
- CVE-2017-7592
- CVE-2017-7593
- CVE-2017-7594
- CVE-2017-7595
- CVE-2017-7596
- CVE-2017-7597
- CVE-2017-7598
- CVE-2017-7599
- CVE-2017-7600
- CVE-2017-7601
- CVE-2017-7602
- CVE-2017-9403

Release date
September 26, 2017

Latest revision
September 26, 2017: 2

Severity
normal

Exploitable
remote

Bugzilla entries

- 610330
- 614020
- 614022
- 617996
- 617998
- 618610
- 624602

Questions or comments?

Please feel free to contact us.