



CVE-2017-7866

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

Summary

CVE	CVE-2017-7866
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-14 04:59:00 UTC
Updated	2017-04-20 17:59:00 UTC
Description	FFmpeg before 2017-01-23 has an out-of-bounds write caused by a stack-based buffer overflow related to the decode_zbu

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
avcodec/pngdec: Fix off by 1 size in decode_zbuf() · FFmpeg/FFmpeg@e371f03 · GitHub	MISC	github.com	Patch, Th
FFmpeg CVE-2017-7866 Stack Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Part
444 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.org	Third Part
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report