CVE-2016-10051

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-10051
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-23 17:59:00 UTC
Updated	2020-11-16 19:57:00 UTC
Description	Use-after-free vulnerability in the ReadPWPImage function in coders/pwp.c in ImageMagick 6.9.5-5 allows remote attackers

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	6.9.5-5	All	All	All
Application	Imagemagick	Imagemagick	6.9.5-5	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All

References

Reference	Source	Link
openSUSE-SU-2017:0399-1: moderate: Security update for GraphicsMagick	SUSE	lists.opensuse.org
openSUSE-SU-2017:0391-1: moderate: Security update for GraphicsMagick	SUSE	lists.opensuse.org
Prevent memory use after free · ImageMagick/ImageMagick@5487013 · GitHub	CONFIRM	github.com
1410456 – (CVE-2016-10051) CVE-2016-10051 ImageMagick: Use after free when using identify or convert	CONFIRM	bugzilla.redhat.co
IM 7.0.2-7 Q16 x86_64 2016-08-04 - Use after free when using identify or convert - ImageMagick	CONFIRM	www.imagemagicl
Prevent memory use after free · ImageMagick/ImageMagick@ecc03a2 · GitHub	CONFIRM	github.com
ImageMagick CVE-2016-10051 Use After Free Denial of Service Vulnerability	BID	www.securityfocus
oss-security - Re: CVE requests for various ImageMagick issues	MLIST	www.openwall.cor

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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