CVE-2017-17879

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

Summary

CVE	CVE-2017-17879
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-27 17:08:21 UTC
Updated	2025-04-20 01:37:25 UTC
Description	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-21, there is a heap-based buffer over-read in ReadOneMNGImage in coder

Risk And Classification

Primary CVSS: v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.013360000 probability, percentile 0.801880000 (date 2026-05-18)

Problem Types: CWE-125 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-16	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
[SECURITY] [DLA 1227-1] imagemagick security update	af854a3a-2127-422b-91ae-364da2661108
Debian -- Security Information -- DSA-4204-1 imagemagick	af854a3a-2127-422b-91ae-364da2661108

USN-3681-1: ImageMagick vulnerabilities | Ubuntu security notices	af854a3a-2127-422b-91ae-364da2661108
ImageMagick CVE-2017-17879 Heap Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108
Debian -- Security Information -- DSA-4074-1 imagemagick	af854a3a-2127-422b-91ae-364da2661108
heap-buffer-overflow in ReadOneMNGImage · Issue #906 · ImageMagick/ImageMagick · GitHub	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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**