

CVE-2016-3714

ImageMagick Improper Input Validation Vulnerability

CISA KEV since Sep 9, 2024

Actively exploited

Public exploit module (Metasploit)

The (1) EPHEMERAL, (2) HTTPS, (3) MVG, (4) MSL, (5) TEXT, (6) SHOW, (7) WIN, and (8) PLT coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to execute arbitrary code via shell metacharacters in a crafted image, aka "ImageTragick."

EVRS 85/100 Immediate priority	CVSS V3.1 8.4 High · NVD	EPSS 0.975 99.9th percentile · FIRST	CISA DEADLINE Sep 30, 2024 KEV since 2024 · listed over a year
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.975 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
imagemagick	≤ 6.9.3-9 7.0.0-0 7.0.1-0	no fixed version listed	NVD
ubuntu linux	12.04 14.04 15.10 16.04	no fixed version listed	NVD
debian linux	8.0 9.0	no fixed version listed	NVD
leap	42.1	no fixed version listed	NVD
opensuse	13.2	no fixed version listed	NVD
suse linux enterprise server	12	no fixed version listed	NVD

Sources

Vendor guidance

www.imagemagick.org/discourse-server/viewtopic.php?f=4&t=29588#p132726, <https://imagemagick.org/archive/releases/>

github.com/advisories/GHSA-24cp-26gx-3pp4
imagemagick.org/discourse-server/viewtopic.php?f=4&t=29588#p132726, <https://imagemagick.org/archive/releases/>
cisa.gov/known-exploited-vulnerabilities-catalog
evulnable.com/vulnerability-management/cve/CVE-2016-3714

Additional guidance imagermagick.com/

NVD nvd.nist.gov/vuln/detail/CVE-2016-3714

CISA KEY

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2016-4735

Current data

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.