

CVE-2016-3718

ImageMagick Server-Side Request Forgery (SSRF) Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

The (1) HTTP and (2) FTP coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to conduct server-side request forgery (SSRF) attacks via a crafted image.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 5.5 Medium · NVD	EPSS 0.756 99.52nd percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.756 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 22 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
imagemagick	< 6.9.3-10 7.0.0-0 7.0.1-0	no fixed version listed	NVD
linux enterprise debuginfo	11	no fixed version listed	NVD
manager	2.1	no fixed version listed	NVD
manager proxy	2.1	no fixed version listed	NVD
openstack cloud	5	no fixed version listed	NVD
enterprise linux desktop	6.0 7.0	no fixed version listed	NVD
enterprise linux eus	6.7 7.2 7.3 7.4 7.5 7.6 7.7	no fixed version listed	NVD
enterprise linux for ibm z systems	6.0 s390x 7.0 s390x	no fixed version listed	NVD

Sources

Vendor guidance	imagemagick.org/discourse-server/viewtopic.php?f=4&t=29588	NVD	nvd.nist.gov/vuln/detail/CVE-2016-3718
CISA KEY	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-4739
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-3718		

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