

CVE-2017-8291

Artifex Ghostscript Type Confusion Vulnerability

CISA KEV since May 24, 2022

Actively exploited

Public exploit module (Metasploit)

Artifex Ghostscript through 2017-04-26 allows -dSAFER bypass and remote command execution via .rsdparams type confusion with a "/OutputFile (%pipe%" substring in a crafted .eps document that is an input to the gs program, as exploited in the wild in April 2017.

EVRS 84 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.970 99.89th percentile · FIRST	CISA DEADLINE Jun 14, 2022 KEV since 2022 · 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	0.970 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
ghostscript	< 9.21	no fixed version listed	NVD
debian linux	8.0	no fixed version listed	NVD
enterprise linux desktop	6.0 7.0	no fixed version listed	NVD
enterprise linux eus	7.3 7.4 7.5 7.6 7.7	no fixed version listed	NVD
enterprise linux server	6.0 7.0	no fixed version listed	NVD
enterprise linux server aus	7.3 7.4 7.6 7.7	no fixed version listed	NVD
enterprise linux server tus	7.3 7.6 7.7	no fixed version listed	NVD
enterprise linux workstation	6.0 7.0	no fixed version listed	NVD

Sources

Vendor guidance bugzilla.redhat.com/show_bug.cgi?id=1446063
NVD nvd.nist.gov/vuln/detail/CVE-2017-8291

Additional guidance access.redhat.com/errata/RHSA-2017:1230
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2017-8291

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-17253

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