

CVE-2013-3346

Adobe Reader and Acrobat Memory Corruption Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

Public exploit module (Metasploit)

Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.

EVRS

81/100

Urgent priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.789

99.6th percentile · FIRST

CISA DEADLINE

Mar 24, 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	0.789 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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
acrobat	≥ 9.0 < 9.5.5 ≥ 10.0 < 10.1.7 ≥ 11.0 < 11.0.03	9.5.5 · 10.1.7 · 11.0.03	NVD
acrobat reader	≥ 9.0 < 9.5.5 ≥ 10.0 < 10.1.7 ≥ 11.0 < 11.0.03	9.5.5 · 10.1.7 · 11.0.03	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-mhw3-773g-72wx	NVD	nvd.nist.gov/vuln/detail/CVE-2013-3346
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2013-3282
Current data	evulnable.com/vulnerability-management/cve/CVE-2013-3346		

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