

CVE-2008-2992

Adobe Reader and Acrobat Input Validation Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a PDF file that calls the util.printf JavaScript function with a crafted format string argument, a related issue to CVE-2008-1104.

EVRS 91/100 Immediate priority	CVSS V3.1 7.8 High · NVD	EPSS 0.998 99.96th 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.998 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately No patch reported by the connected remediation source

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
acrobat	≤ 8.1.2	after 8.1.2	NVD
acrobat reader	≤ 8.1.2	after 8.1.2	NVD
solaris	10	no fixed version listed	NVD

Sources

NVD nvd.nist.gov/vuln/detail/CVE-2008-2992

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2008-2982

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2008-2992

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