

CVE-2021-28550

Adobe Acrobat and Reader Use-After-Free Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

EVRS 75_{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.519 99th percentile · FIRST	CISA DEADLINE Nov 17, 2021 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	0.519 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ 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 dc	≥ 15.008.20082 ≤ 21.001.20150 ≥ 15.008.20082 ≤ 21.001.20149	after 21.001.20150	NVD
acrobat reader dc	≥ 15.008.20082 ≤ 21.001.20150 ≥ 15.008.20082 ≤ 21.001.20149	after 21.001.20150	NVD
acrobat	≥ 17.011.30059 ≤ 17.011.30194 ≥ 20.001.30005 ≤ 20.001.30020	after 17.011.30194 · after 20.001.30020	NVD
acrobat reader	≥ 17.011.30059 ≤ 17.011.30194 ≥ 20.001.30005 ≤ 20.001.30020	after 17.011.30194 · after 20.001.30020	NVD
windows	—	no fixed version listed	NVD
macos	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-865h-4rjv-52pg

Additional guidance helpx.adobe.com/security/products/acrobat/apsb21-29.html

NVD nvd.nist.gov/vuln/detail/CVE-2021-28550

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-15226

Current data evulnable.com/vulnerability-management/cve/CVE-2021-28550

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