

CVE-2024-4978

Justice AV Solutions (JAVS) Viewer Installer Embedded Malicious Code Vulnerability

CISA KEV since May 29, 2024

Actively exploited

Justice AV Solutions Viewer Setup 8.3.7.250-1 contains a malicious binary when executed and is signed with an unexpected authenticode signature. A remote, privileged threat actor may exploit this vulnerability to execute of unauthorized PowerShell commands.

EVRS 75/100 Urgent priority	CVSS V4.0 8.7 High · NVD	EPSS 0.269 98th percentile · FIRST	CISA DEADLINE Jun 19, 2024 KEV since 2024 · 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	0.269 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.7	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA note:** Please follow the vendor's instructions as outlined in the public statements at <https://www.rapid7.com/blog/post/2024/05/23/cve-2024-4978-backdoored-justice-av-solutions-viewer-software-used-in-apparent-supply-chain-attack#remediation> and <https://www.javs.com/downloads>
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
javs viewer	8.3.7.250	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-wf54-f8v9-v72v	NVD	nvd.nist.gov/vuln/detail/CVE-2024-4978
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-44535
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-4978		

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