

CVE-2021-27852

Checkbox Survey Deserialization of Untrusted Data Vulnerability

CISA KEV since Apr 11, 2022

Actively exploited

Deserialization of Untrusted Data vulnerability in CheckboxWeb.dll of Checkbox Survey allows an unauthenticated remote attacker to execute arbitrary code. This issue affects: Checkbox Survey versions prior to 7.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.303 98.2nd percentile · FIRST	CISA DEADLINE May 2, 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	0.303 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: Versions 6 and earlier for this product are end-of-life and must be removed from agency networks. Versions 7 and later are not considered vulnerable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
survey	< 7.0	7.0	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-xrx4-vq84-23w6	NVD	nvd.nist.gov/vuln/detail/CVE-2021-27852
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-14590
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-27852		

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