

CVE-2019-10758

MongoDB mongo-express Remote Code Execution Vulnerability

CISA KEV since Dec 10, 2021

Actively exploited

mongo-express before 0.54.0 is vulnerable to Remote Code Execution via endpoints that uses the `toBSON` method. A misuse of the `vm` dependency to perform `exec` commands in a non-safe environment.

EVRS 83 / ₁₀₀ Urgent priority	CVSS V3.1 9.9 Critical · NVD	EPSS 0.847 99.71st percentile · FIRST	CISA DEADLINE Jun 10, 2022 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	0.847 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.9	☐ 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
mongo-express	< 0.54.0	0.54.0	GitHub

Sources

Vendor guidance	github.com/advisories/GHSA-h47j-hc6x-h3qq	NVD	nvd.nist.gov/vuln/detail/CVE-2019-10758
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-0791
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-10758		

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