

CVE-2021-41277

Metabase GeoJSON API Local File Inclusion Vulnerability

CISA KEV since Nov 12, 2024

Actively exploited

Metabase is an open source data analytics platform. In affected versions a security issue has been discovered with the custom GeoJSON map (`admin->settings->maps->custom maps->add a map`) support and potential local file inclusion (including environment variables). URLs were not validated prior to being loaded. This issue is fixed in a new maintenance release (0.40.5 and 1.40.5), and any subsequent release after that.

EVRS 84 /100 Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.972 99.9th percentile · FIRST	CISA DEADLINE Dec 3, 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	Added to CISA KEV within the last two years
☒ EPSS	0.972 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ 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.

Basis: CISA KEV required action

If you're unable to upgrade immediately, you can mitigate this by including rules in your reverse proxy or load balancer or WAF to provide a validation filter before the application.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
metabase	0.40.0 0.40.1 0.40.2 0.40.3 0.40.4 1.40.0 1.40.1 1.40.2 1.40.3 1.40.4	no fixed version listed	NVD

Sources

Vendor guidance github.com/metabase/metabase/commit/042a36e49574c749f944e19cf80360fd3dc322f0**NVD** nvd.nist.gov/vuln/detail/CVE-2021-41277**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2021-28310**github.com** github.com/metabase/metabase/security/advisories/GHSA-w73v-6p7p-fpfr**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**Current data** evulnable.com/vulnerability-management/cve/CVE-2021-41277

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