# SSRF in Metabase GeoJSON URL

Medium

← View More Research Advisories

## Synopsis

A researcher at Tenable discovered an SSRF vulnerability in Metabase < 44.5.

**Background**

There is a feature in the /api/geojson endpoint of Metabase which will make a web request to a user-specified url on behalf of an authenticated user. This was reported as an SSRF vulnerability in 2021 as CVE-2021-41277. Metabase released a patch to prevent the loading of local files, and blacklist a number of specific hosts related to metadata endpoints for cloud-hosted Metabase instances.

Unfortunately, that patch did not account for 301 or 302 redirect responses, so the blacklist of such metadata endpoints could be circumvented.

**Details**

The blacklisting of link-local addresses can be circumvented using HTTP 301/302 redirects. Directing the url parameter to an attacker-controlled site which responds with a 301 or 302 redirect to an otherwise blocked ip address/domain allows an attacker to bypass the mitigation for CVE-2021-41277.

**Proof of Concept:**
Attempting to navigate to **http://<metabaseHost>:3000/api/geojson?url=http://metadata.google.internal** results in the error message:
**Invalid GeoJSON file location: must either start with http:// or https://...etc**

However, navigating to an attacker controlled page **http://<metabaseHost>:3000/api/geojson?url=http://attackerServer.example/** which responds with the following 302 response:

will redirect Metabase to the prohibited address (in this case, **http://metadata.google.internal/**), potentially allowing an attacker to reveal sensitive information.

## Solution

Metabase has addressed the redirect issue in Metabase version 44.5

## Additional References

https://github.com/metabase/metabase/security/advisories/GHSA-w5j7-4mgm-77f4
https://nvd.nist.gov/vuln/detail/CVE-2021-41277

## Disclosure Timeline

15 September 2022 - Issue reported to Metabase
16 September 2022 - Issue confirmed by Metabase
7 October 2022 - Tenable inquires whether there have been any updates
25 October 2022 - Metabase responds, noting that a patch has been released.

*All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.*

*Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.*

*For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.*

*If you have questions or corrections about this advisory, please email advisories@tenable.com*

## Risk Information

**CVE ID:** CVE-2022-43776
**Tenable Advisory ID:** TRA-2022-34
**Credit:** Ronan Donohue
**CVSSv3 Base / Temporal Score:** 4.3
**CVSSv3 Vector:** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
**Affected Products:** Metabase < 44.5

25 October 2022 - Advisory published

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security

Compliance

Exposure Management

Finance

Healthcare

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

## CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

## CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media