Adminer Server Side Request Forgery (SSRF)

Adam Crosser
Brian Sizemore

Description:

We have discovered a way to use adminer to send arbitrary get requests and retrieve JSON responses from internal servers. Specifically, this was demonstrated in order to extract AWS access keys from the AWS metadata service.

Impact:

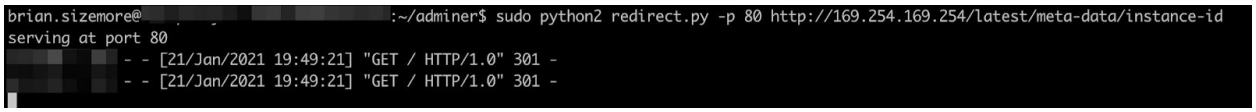
The impact of this finding will be dependent upon the sensitivity of resources available on the internal network. Theoretically, an attacker could automate the use of this vulnerability to perform some “scanning” activities and enumerate the internal environment. In the case of an AWS server, the impact will likely be related to the permissions granted to the server and an attacker’s ability to escalate or move laterally with the compromised AWS keys.

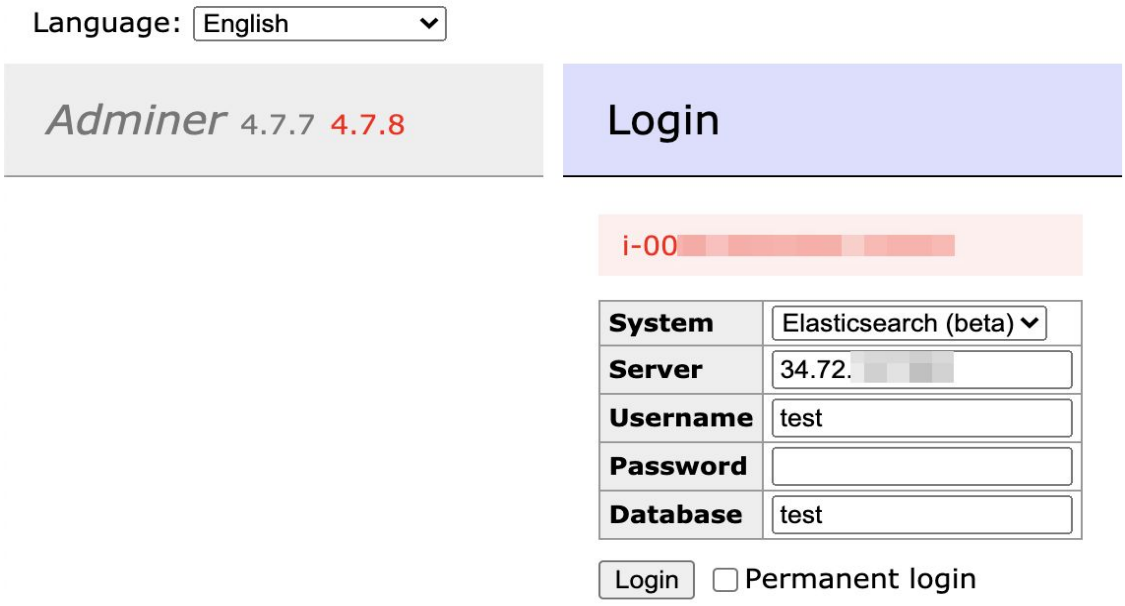
Attack Explanation and Demonstration:

The following steps were used to demonstrate the attack.
First, a python server was started which listened for incoming connections and responded with a 301 redirect to an arbitrarily chosen host. In this example case, the redirect was pointed at the AWS metadata service:
http://169.254.169.254/latest/meta-data/instance-id

Then the Elasticsearch login module was used within Adminer to “login” to the server running the python code which resulted in Adminer printing the json response from the metadata server containing the server’s AWS instance-id. The screenshots below demonstrate the successful attack.

A copy of the python script used to redirect the request can be found here:
https://gist.github.com/bpsizemore/227141941c5075d96a34e375c63ae3bd





In order to demonstrate the potential severity of impact, the redirect was also used to list the available roles for the server at
http://169.254.169.254/latest/meta-data/iam/security-credentials/
before extracting the keys by navigating to one of the available rolls.
The screenshot below shows the result of navigating to one of the available rolls.