Unsecured Credentials: Cloud Instance Metadata API, Sub-technique T1552.005 - Enterprise

Archived: 2026-04-05 12:52:08 UTC

Adversaries may attempt to access the Cloud Instance Metadata API to collect credentials and other sensitive data.

Most cloud service providers support a Cloud Instance Metadata API which is a service provided to running virtual instances that allows applications to access information about the running virtual instance. Available information generally includes name, security group, and additional metadata including sensitive data such as credentials and UserData scripts that may contain additional secrets. The Instance Metadata API is provided as a convenience to assist in managing applications and is accessible by anyone who can access the instance.[1] A cloud metadata API has been used in at least one high profile compromise.[2]

If adversaries have a presence on the running virtual instance, they may query the Instance Metadata API directly to identify credentials that grant access to additional resources. Additionally, adversaries may exploit a Server-Side Request Forgery (SSRF) vulnerability in a public facing web proxy that allows them to gain access to the sensitive information via a request to the Instance Metadata API.[3]

The de facto standard across cloud service providers is to host the Instance Metadata API at `http[:]//169.254.169.254`.

Source: https://attack.mitre.org/techniques/T1552/005