

IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020

Legend

AWS API Call



AWS

gotcha np, we got encryption and what not



AWS Systems Manager

Attacker's AWS Account

Subnet



Victim

Let's store this secret in a secure place

Notes

1. From this point on the victim will use the attacker's credential's when issuing API calls to AWS.
2. Requests will fail with API calls that require an ARN, or certain expectations are made about the environment that don't match the attacker's account.
3. But if the attacker is lucky then the user may use an API call that is vulnerable, such as SSM PutParameter. In which case the content/secret is uploaded to the attacker's account.

IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020

AWS



Victim's AWS Account

Legend

API Call



API Response



Subnet



100t b0x

can I Haz s3cr3t



Attacker

AWS

i mean, sure, it's your
account, right?



AWS Systems
Manager

Attacker's AWS Account

Notes

1. **Uploaded content can than be retrieved by the attacker, regardless of if it's (server side) encrypted or not.**
2. *In this specific example using a non-default KMS key however would have mitigated the issue. This is simply due to the API call requiring an ARN rather than a relative path.*
3. *However if the ARN is constructed through a get-caller-identity call, which is vulnerable to this attack. It becomes possible (with a good bit of luck and skill!) for this attack to work again, despite a non-default KMS key being used.*