CWL
CyberWarFare Labs

An Analysis of Public AWS AMI Security Risks

Insights on Public AWS AMI Security Risks and Best Practices

About CyberWarFare Labs :

CW Labs is a renowned Infosec company specializing in cybersecurity practical learning. They provide on-demand educational services. The company has 3 primary divisions :

1. Learning Management System (LMS) Platform

2. CWL CyberSecurity Playground (CCSP) Platform

3. Infinity Learning Platform

About Me

> Security Intern at CW Labs.

> Googles ‘*How to not mess up a webinar*’ and still ends up doing it anyway

What we will cover in today's brief session

1. Case study overview
2. Impact of the incident
3. Lessons Learnt and Best practices
4. AMA Session

1

CASE STUDY OVERVIEW

- Researchers discovered sensitive data like API keys and credentials in public Amazon Machine Images (AMIs) on AWS.
- The exposure was due to misconfigured cloud resources.
- Sensitive information was carelessly or inadvertently kept in AMIs.
- Improper cleanup before making AMIs public led to the risk.

- Developers or organizations failed to remove configuration files.
- Environment variables were not cleared before making AMIs public.
- Hardcoded credentials were left in public AMIs.
- The discovery highlighted the need for proper AMI security practices.

2

IMPACT OF THE INCIDENT

- **Data Breaches:** Sensitive data like API keys and credentials were exposed, leading to unauthorized access.

- **Financial Losses**: Stolen credentials could be used for costly cloud services, causing unexpected bills.

- **Reputation Damage**: Customer trust was eroded, and brand reputation suffered due to public exposure.

- **Regulatory Issues**: Exposed data violated regulations like GDPR and HIPAA, risking fines and legal action.

- **Increased Attack Surface**: Exposed credentials allowed attackers to escalate privileges and access more resources.

- **Loss of Intellectual Property**: Sensitive code and data could be stolen for financial or competitive advantage.

3

LESSONS LEARNT AND BEST PRACTICES

- **Limit Public AMIs**: Use public AMIs only when absolutely necessary; default to private AMIs to reduce exposure.

- **Sensitive Data Cleanup**: Always remove sensitive information, such as credentials, before making AMIs public.

- **Secrets Management**: Use secure tools like AWS Secrets Manager or HashiCorp Vault to manage credentials safely.

- **Educate Teams**: Train developers and cloud engineers on secure coding practices and the risks of exposing sensitive data.

- **Use Private AMIs**: Default to private AMIs and restrict access with IAM policies to authorized users.

- **Automate Secrets Detection**: Use tools like TruffleHog or AWS Macie to scan for exposed secrets in AMIs.

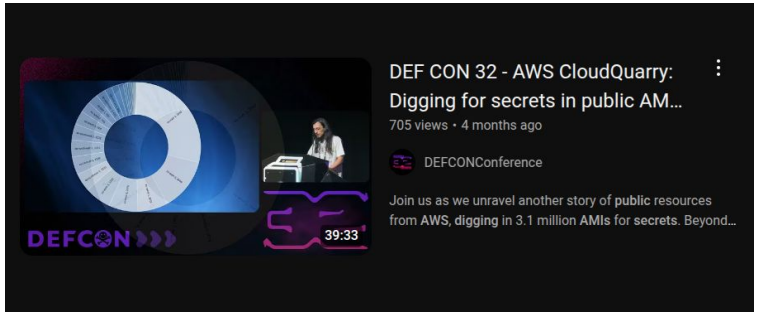
- **Enforce Least Privilege**: Implement strict IAM policies, ensuring minimal permissions for users and services.

- **Encrypt Sensitive Data**: Encrypt sensitive data stored in AMIs to ensure it remains protected even if exposed.

AWS CloudQuarry: Digging for Secrets in Public AMIs

Money, secrets and mass exploitation: This research unveils a quarry of sensitive data stored in public AMIs. Digging through each AMI we managed to collect 500 GB of credentials, private repositor…

37 min. read



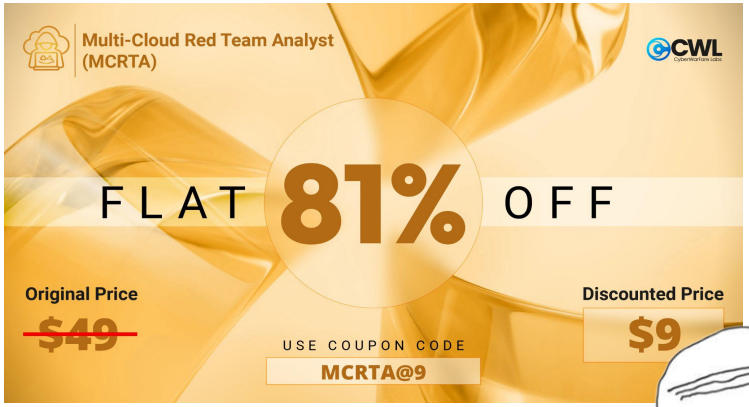
AWS CloudQuarry: Digging for Secrets in Public AMIs – Security Café

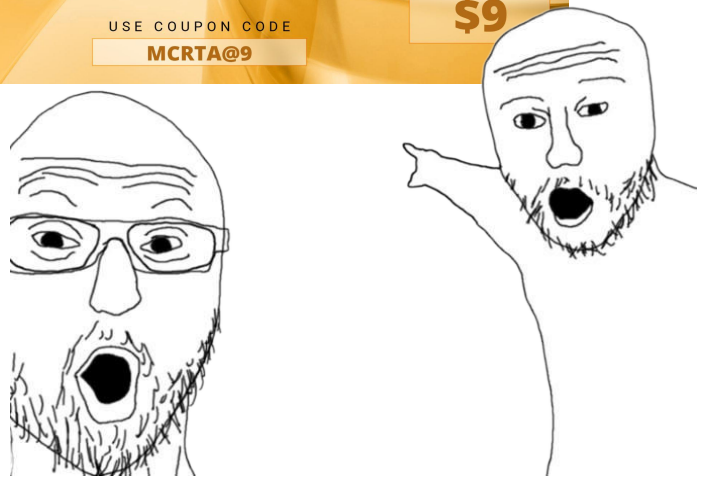
DEF CON 32 – Eduard Agavriloae, Matei Josephs – YouTube

4

ASK ME ANYTHING!

Now is a great opportunity to interact with the CWL team.
If you have any questions or queries regarding the courses, exams, or anything related to cybersecurity,
Feel free to ask!





PS: We're offering a huge 81% discount on the Multi-Cloud Red Team Analyst (MCRTA) course. Take advantage of this offer while it lasts