IMPORTANT CYBERSECURITY NEWS: WHOAMI ATTACKS GIVE HACKERS CODE EXECUTION ON AMAZON EC2 INSTANCES

Vairav Cyber Security News Report

Date: 2025-02-14

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity incident has revealed a vulnerability in Amazon Web Services (AWS) that could allow attackers to execute code within AWS Elastic Compute Cloud (EC2) instances. Researchers from Datadog identified a “name confusion” attack, dubbed “whoAMI,” where malicious actors can exploit misconfigurations in retrieving Amazon Machine Image (AMI) IDs. This vulnerability arises when organizations search for AMIs without specifying the ‘owners’ attribute, potentially leading to the selection of malicious images. AWS has acknowledged the issue and introduced measures to mitigate the risk.

DETAILS OF THE INCIDENT

Description: The “whoAMI” attack is a name confusion vulnerability targeting AWS’s community AMI catalog. Attackers can publish a malicious AMI with a name that closely resembles legitimate images. When organizations search for AMIs without specifying the ‘owners’ attribute, they risk selecting these malicious images. Once deployed, these compromised AMIs can grant attackers code execution capabilities within the victim’s AWS environment.

Identification: Datadog’s Security Labs identified this pattern in August 2024 while analyzing how various software projects retrieve AMIs for creating EC2 instances. They discovered that omitting the ‘owners’ attribute during the AMI search process could lead to the selection of malicious images.

Affected Entities/Industries: Organizations utilizing AWS EC2 instances and retrieving AMIs without specifying the ‘owners’ attribute are at risk. This vulnerability can affect various industries relying on AWS for cloud services.

Potential Impact: Exploiting this vulnerability can lead to unauthorized code execution within an organization’s AWS environment, resulting in data breaches, system compromises, and potential financial and reputational damage.

Exploitation Methods: Attackers create malicious AMIs with names mimicking legitimate images. When organizations search for AMIs without the 'owners' attribute, they may inadvertently select these malicious images, leading to system compromise upon deployment.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Specify the 'owners' attribute when searching for AMIs to ensure selection from trusted sources.
- Review and update existing configurations to include the 'owners' attribute in AMI searches.
- Implement AWS's "Allowed AMIs" feature to restrict the use of AMIs to those from trusted accounts.

Security Best Practices

- Regularly audit AWS configurations and usage to identify and remediate potential vulnerabilities.
- Educate development and operations teams on the importance of specifying the 'owners' attribute during AMI searches.
- Monitor AWS environments for unauthorized or unusual activity, especially related to EC2 instances.

For Advanced Security Teams

- Deploy intrusion detection systems to monitor for anomalous behaviors within AWS environments.
- Conduct regular threat hunting exercises focusing on cloud infrastructure vulnerabilities.
- Collaborate with AWS support and security communities to stay updated on emerging threats and mitigation strategies.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://securitylabs.datadoghq.com/articles/whoami-a-cloud-image-name-confusion-attack/
- https://www.bleepingcomputer.com/news/security/whoami-attacks-give-hackers-code-execution-on-amazon-ec2-instances/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com