CWL
CyberWarFare Labs

FROM HEAP DUMPS TO AWS SECRET

THE DARK SIDE OF SPRING BOOT EXPOSURE

ABOUT CYBERWARFARE LABS :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform

aws
Cloud Security
RED TEAM
PURPLE TEAM
BLUE TEAM
AD
WEB
On-Premise Security
CI/CD
PLATFORM
NETWORK

INFINITE LEARNING EXPERIENCE

ABOUT SPEAKER

SUBASHINI K B

Security Consultant

Subashini Balaji is a Security Consultant at **CyberWarFare Labs**, specializing in **Red Teaming and APT simulations** in enterprise environments. She also writes **technical blogs and articles** focused on real-world cyber attack techniques and defenses.

Agenda for the Day

- What is Spring Boot Actuator?
- What is a Heap Dump?
- Why Is a Heap Dump Dangerous?
- Prevention
- ATTACK FLOW
- Practical Demo

What is Spring Boot Actuator?

- **Spring Boot Actuator** is a powerful tool that provides **production-ready features** to help you monitor and manage your Spring Boot applications.

- It exposes a variety of **REST endpoints** that offer insights into the application's **health, metrics, environment settings** and more making it easier to debug, monitor and maintain applications in real-time.

- If Actuator endpoints are **exposed to the internet without proper authentication or access control**, they can be exploited by attackers to gather sensitive information

What is a Heap Dump?

- ❖ A **heap dump** is a **snapshot of the memory heap** of a Java application at a specific moment in time.
- ❖ The heap is the area of memory used to store **Java objects during the runtime** of the application.

Heap Dump May Contain :

1. Cloud Access Credentials
2. Secrets & API Keys
3. Environment Variables
4. Configuration Properties
5. Session Data
6. Cached Data
7. Sensitive Metadata URLs
8. Logs and Debug Information

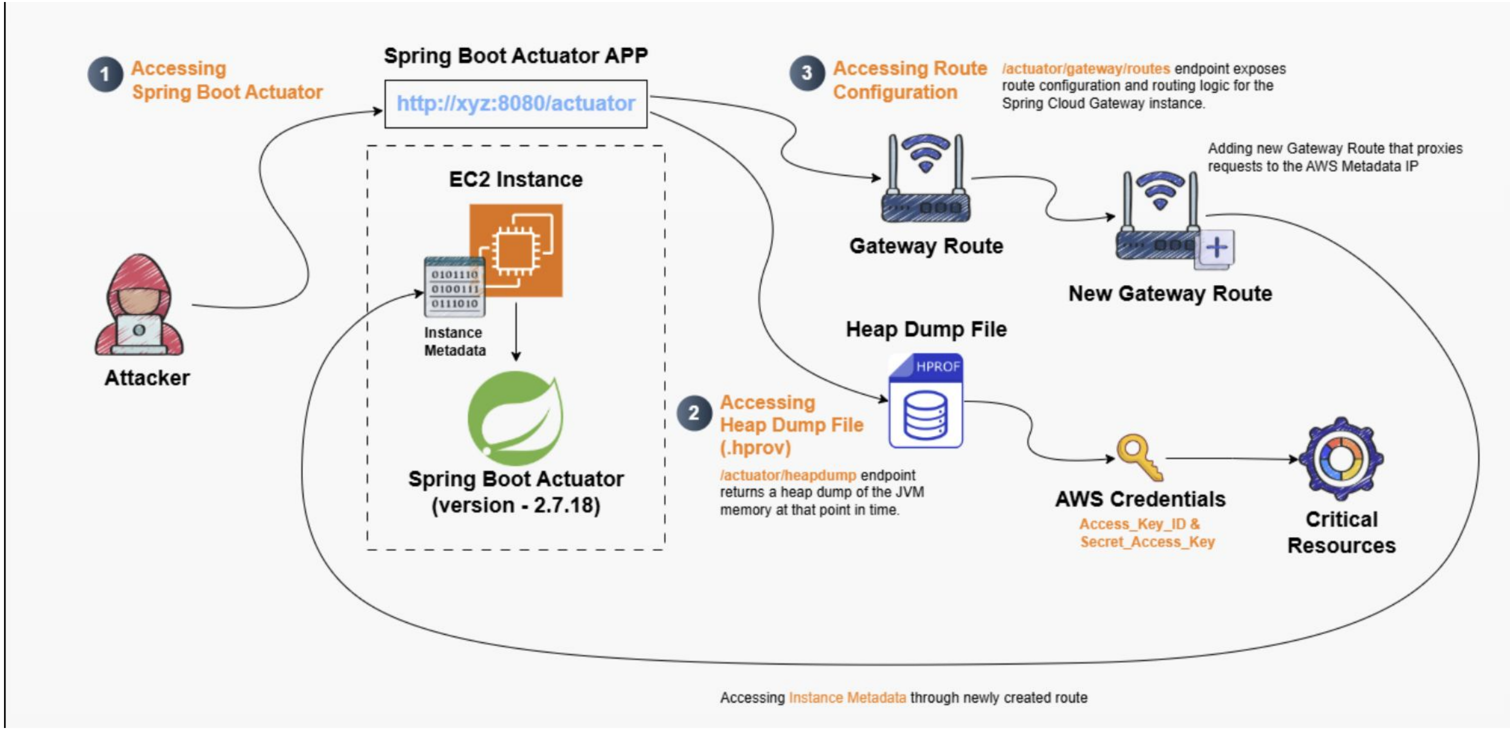
Why Is a Heap Dump Dangerous?

- It can contain sensitive data like:
  - API keys
  - Database passwords
  - Session tokens
  - Plaintext secrets
- Attackers can find user data or even CTF flags hidden in memory.
- It shows how the app works internally, which helps attackers find more ways to exploit it.

How to prevent spring boot actuator?

- **Never expose actuator endpoints publicly.**
- **Disable unused endpoints**.
- **Use authentication** with Spring Security and roles like **ACTUATOR_ADMIN**.
- **Monitor logs** for suspicious access to /actuator paths.
- **Block metadata IP** access from the app layer.
- **For AWS**, enforce **IMDSv2** and use **firewall rules** to restrict metadata access.

ATTACK FLOW



Spring Boot Actuator APP

http://xyz:8080/actuator

1 Accessing Spring Boot Actuator

Attacker

EC2 Instance

Instance Metadata

Spring Boot Actuator (version - 2.7.18)

2 Accessing Heap Dump File (.hprov)

/actuator/heapdump endpoint returns a heap dump of the JVM memory at that point in time.

Heap Dump File

HPROF

3 Accessing Route Configuration

/actuator/gateway/routes endpoint exposes route configuration and routing logic for the Spring Cloud Gateway instance.

Gateway Route

Adding new Gateway Route that proxies requests to the AWS Metadata IP

New Gateway Route

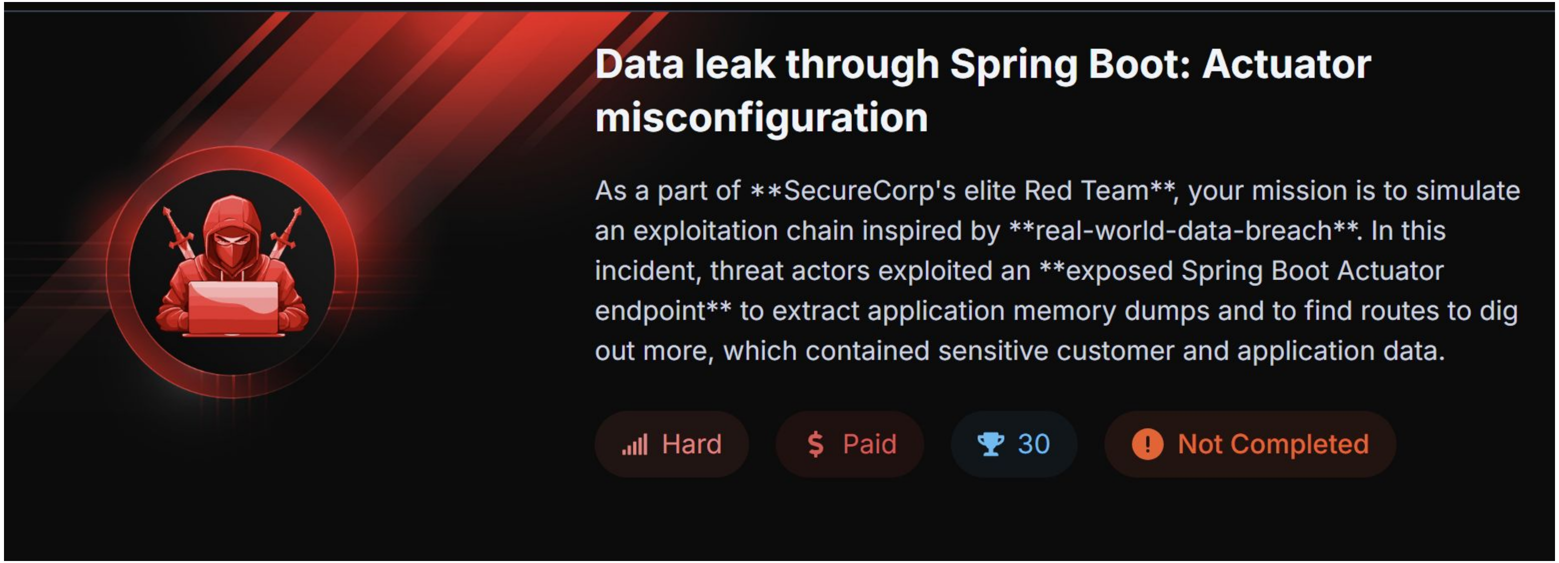
AWS Credentials

Access_Key_ID & Secret_Access_Key

Critical Resources

Accessing Instance Metadata through newly created route

SOLVING CHALLENGE



Data leak through Spring Boot: Actuator misconfiguration

As a part of **SecureCorp's elite Red Team**, your mission is to simulate an exploitation chain inspired by **real-world-data-breach**. In this incident, threat actors exploited an **exposed Spring Boot Actuator endpoint** to extract application memory dumps and to find routes to dig out more, which contained sensitive customer and application data.

CWL
CyberWarFare Labs

100% OFF

CWL INFINITY LEARNING PLATFORM

WORTH $29

GET ONE MONTH FREE ACCESS OF PLATFORM

PAID CHALLENGES

ACCESS TO FRESH LABS WEEKLY

AVAIL ANYTIME

USE COUPON CODE

INFINITYACCESS

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **https://cyberwarfare.live**