# Log4J Vulnerabilities - Amazon Resolutions (Updated to 10 Dec 2021)

The information provided below is referred from https://aws.amazon.com/security/security-bulletins/AWS-2021-006/.

- **CVE Number**

  2021-44228
  2021-45046

- **Discovery Date**

  Dec 10, 2021

- **Threat Level**

  High

- **Response to Log4j**

AWS is aware of the recently disclosed issues relating to the open-source Apache “Log4j2″ utility (CVE-2021-44228 and CVE-2021-45046).

Responding to security issues such as this one shows the value of having multiple layers of defensive technologies, which is so important to maintaining the security of our customers’ data and workloads. They have taking this issue very seriously, and our world-class team of engineers have been working around the clock on our response and remediation. They expect to rapidly restore our full state of defense in depth.

One of the technologies we’ve developed and deployed extensively inside AWS is a hot patch for applications that may include Log4j. This hot patch updates the Java VM to disable the loading of the Java Naming and Directory Interface (JNDI) class, replacing it with a harmless notification message, which is an effective mitigation of CVE-2021-44228 and CVE-2021-45046.

- **Affected Amazon Products**

Most of the Amazon Product has been affected by Log4j vulnerabilities as the following:

1. Amazon EKS
2. Amazon ECS
3. Amazon Fargate

The customer need to apply the hotfix to fix

- **The following Amazon Product has been updated to mitigate the issues identified in CVE-2021-44228**

1. Amazon Cognito
2. Amazon Pinpoint
3. Amazon Event Bridge

4. Amazon Load Balancing
5. AWS Route 53