QualityNet | AWS Cloud

December 22, 2021

EMR log4js Mitigation

FOR IMMEDIATE RELEASE

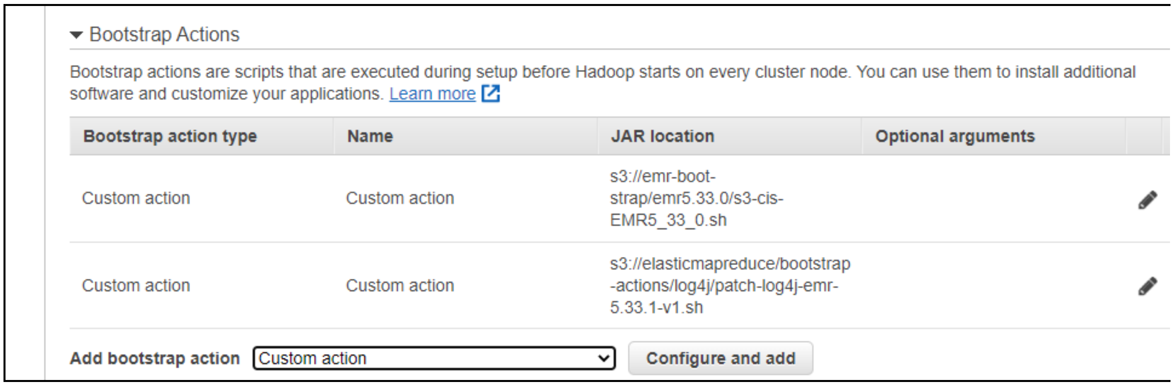
The following procedure provides instructions for mitigation of the log4js exploit in Elastic Map Reduce (EMR) Clusters in light of some unclear language in the current AWS documentation.

- AWS's documentation suggests that for some versions of EMR, the mitigation script requires EMR 6.x.1 and 5.x.1 to be applied.
- However, the HIDS Cloud Team has confirmed with AWS Support that this is not a necessity. The HIDS Cloud Team has tested on CMS approved versions of EMR and confirmed the mitigation technique is successful as long as the major and minor versions match, for example: 5.33 and 6.3.

ADOs using the EMR Cluster Service should follow the directions in the existing Ventech EMR launch procedures.

For example:

- Launch an EMR 5.33.0 cluster in the normal fashion by calling VT Hardening Script for EMR 5.33.0 from the S3 URI: s3://emr-boot-strap/emr5.33.0/s3-cis-EMR5_33_0.sh
  - Ref: https://qnetconfluence.cms.gov/display/HIDS/EMR+Cluster+Configuration
- Additionally calling the AWS provided log4js mitigation script s3://elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.33.1-v1.sh during bootstrap.
  - Ref: https://docs.aws.amazon.com/emr/latest/ReleaseGuide/emr-log4j-vulnerability.html

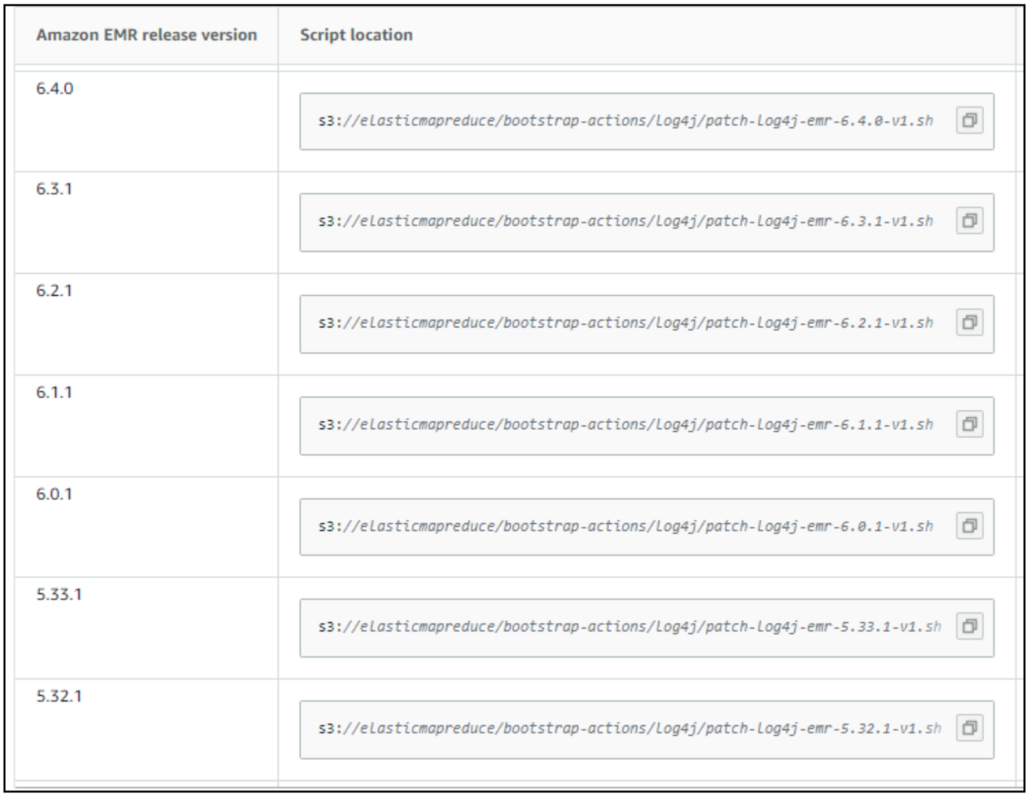


Bootstrap Actions

Bootstrap actions are scripts that are executed during setup before Hadoop starts on every cluster node. You can use them to install additional software and customize your applications. Learn more

Bootstrap action type	Name	JAR location	Optional arguments
Custom action	Custom action	s3://emr-boot-strap/emr5.33.0/s3-cis-EMR5_33_0.sh	
Custom action	Custom action	s3://elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.33.1-v1.sh	

Add bootstrap action: Custom action



Amazon EMR release version	Script location
6.4.0	`s3://elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-6.4.0-v1.sh`
6.3.1	`s3://elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-6.3.1-v1.sh`
6.2.1	`s3://elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-6.2.1-v1.sh`
6.1.1	`s3://elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-6.1.1-v1.sh`
6.0.1	`s3://elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-6.0.1-v1.sh`
5.33.1	`s3://elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.33.1-v1.sh`
5.32.1	`s3://elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.32.1-v1.sh`

NOTES:

- AWS Support recommends that the log4j remediation scripts should be applied and tested on EMR in lower environments before use in production.
- Tenable scans and reports for the presence of vulnerable versions .jar files.
- The recommendation from HIDS Security Engineering is to delete the offending jar files if possible.
- If Tenable does identify vulnerable jar files, an analysis of the specific EMR deployment will have to be done by the ADOs for possible functional impact should the flagged jar file(s) be deleted. If it is determined that a negative impact will occur an exception will have to be submitted to the CMS ISSO for approval.

If you need additional information, please contact us by phone at 1-866-288-8914, Slack at #help-service-center-sos, or by email at ServiceCenterSOS@cms.hhs.gov.

CMS.gov