Zenoss update on the Apache Log4j CVE-2021-44228 vulnerability

Zenoss has completed an assessment of the impact of the log4j vulnerability recently identified as CVE-2021-44228 to all of our cloud and on-premise products including Zenoss Cloud, Zenoss as a Service (ZaaS), Zenoss Service Dynamics (Resource Manager, Impact, Analytics), all associated collectors, and all ZenPacks and integrations.

For customers using Zenoss Cloud

Although Zenoss Cloud does use technologies running log4j, we have determined that our customers are not currently affected or exposed by this vulnerability as Zenoss Cloud does not use or enable the particular feature of the log4j package that causes the vulnerability. Zenoss is following the CISA advice to apply a further mitigation step found here to all Cloud environments. Cloud Collectors do not run log4j so are not affected. No action is required by our customers.

For our on-premise customers using Zenoss Service Dynamics (Resource Manager, Impact, Analytics)

Not currently affected or exposed by this vulnerability. Here is a breakdown by product:

- Resource Manager 4.x - not affected
- Resource Manager 5.x - not affected
- Resource Manager 6.x - Zenoss does not use or enable the particular feature of the log4j package that causes the vulnerability. However, Zenoss strongly recommends that all on-premise customers immediately take the following steps to improve mitigation.

  To mitigate CVE-2021-44228 for Solr, perform the following steps:

  1. In Control Center, navigate to Infrastructure/Solr service of your deployed Zenoss application.
  2. Click on Edit for the /opt/solr/zenoss/etc/solr.in.sh Configuration File.
  3. Add the line `SOLR_OPTS="$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true"`
  4. Click Save
  5. Restart the Solr service.

- Impact - No log4j files are used for this product.
- Control Center - Not affected by the vulnerability.
- Analytics - No impact, but customers can further mitigate by taking the below steps:

  To mitigate CVE-2021-44228 in Analytics:

  1. Ssh to the Analytics server as root

2. Switch to the directory containing the library code files
   `# cd /opt/zenoss_analytics/webapps/etl/WEB-INF/lib`
3. Run the following command
   `# zip -q -d log4j-core-2.6.2.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`
4. Restart Analytics: `# service zenoss_analytics restart`

For hosted customers using Zenoss as a Service (ZaaS)

Not currently affected or exposed by this vulnerability. Since ZaaS is a hosted version of Zenoss Service Dynamics, the further mitigation steps listed above will be applied by Zenoss. No action is required by our customers.