Zenoss update on the Apache Log4j CVE-2021-44228 vulnerability
December 20, 2021 v1.2 Update

Change Log

Date	Version	What changed
12/14/21	v1.0	No changes
12/16/21	v1.1	Updated Resource Manager v6.x mitigation steps to reflect updated Apache CVE mitigation guidance.
12/17/21	v1.2	1. Updated affected versions of Resource Manager v6.x. 2. Corrected error in Resource Manager v6.x mitigation step #9. Was “service”, now “snapshot”. 3. Outlined Control Center patch plan for affected Elastic and Logstash.

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 6.0 to 6.5 - Not affected as these versions use log4j 1.x that does not have this vulnerability.
- Resource Manager **6.6 only** - 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. SSH to the "master" server where Control Center is running.
2. Create a backup snapshot
   `serviced service snapshot Zenoss.resmgr --tag $(date +%Y%m%d)_presolrlog4jfix`
3. Start a container. Changes in this container will be used to update the image.
   `serviced service shell -i --saveas solrlog4jfix solr`
4. Change directory to Solr's library files
   `cd /opt/solr/server/lib/ext`
5. Apply the Log4j vulnerability mitigation
   `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`
6. Change to another directory of Solr's library files
   `cd /opt/solr/contrib/prometheus-exporter/lib`
7. Apply the Log4j vulnerability mitigation
   `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`
8. Exit the container
   `exit`
9. Commit the changes
   `serviced snapshot commit solrlog4jfix`
10. Restart the Zenoss application (all the services).

- Impact - No log4j files are used for this product.
- Control Center - Elastic uses the vulnerable version of log4j in both the general Elastic software and Logstash. Per Elastic (scroll to Dec 18 update) the vulnerability is not exploitable. Regardless, we will be providing a patch for Control Center 1.9.0 that will update Elastic and Logstash to the most current log4j 2.x versions. We are targeting this CC patch availability by the end of this week (Dec 24). As soon as it is available, we will update you.
- 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.

References

Elastic guidance URL linked above
https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476

Updated Apache guidance URL linked above
https://logging.apache.org/log4j/2.x/security.html