eG Enterprise and Log4jShell/Logback Vulnerabilities: Update

A Security Advisory

Updated on 22nd Dec 2021

About the Log4jShell Vulnerability

As reported widely, a new remote code execution (RCE) vulnerability, CVE-2021-44228 (also called Log4jShell) has been found in the widely used the Apache Log4j java library. For more details on this vulnerability, please see https://www.theverge.com/2021/12/10/22828303/log4j-library-vulnerability-log4shell-zero-day-exploit. This is a vulnerability classified under the highest severity mark, i.e., 10 out of 10.

Please note that this vulnerability attacks Java-based web applications that use the following software components (https://www.veracode.com/blog/security-news/urgent-analysis-and-remediation-guidance-log4j-zero-day-rce-cve-2021-44228):

- Log4j version – all 2.x versions prior to 2.16.0, AND
- JVM version - if lower than:
    - Java 6 – 6u212
    - Java 7 – 7u202
    - Java 8 – 8u192
    - Java 11 - 11.0.2

eG Enterprise versions up to v7.1.8 use Log4j v1, not Log4j v2. Log4j v1 does not have the JndiLookup class that is the source of this vulnerability – see https://blog.cloudflare.com/inside-the-log4j2-vulnerability-cve-2021-44228/. One can review the difference in risk level of attacks between Log4j v1 and v2 here - https://www.horizon3.ai/cve-2021-44228/. The risk level further reduces if the JRE used for the application is recent.

Our security team has tested eG Enterprise using community provided test cases for CVE-2021-44228. We have also used the Huntress Log4Shell Vulnerability Tester - https://log4shell.huntress.com, and **we have not found any evidence that eG Enterprise v7.1.4 to v7.1.8 is vulnerable to Log4jShell**.

About the Logback Vulnerability

Another logging library used by eG Enterprise is logback. As indicated in http://slf4j.org/log4shell.html, Logback does NOT offer a lookup mechanism at the message level. Thus, it is deemed safe with respect to CVE-2021-44228.

However, logback may make JNDI calls from within its configuration file. This was recently reported in LOGBACK-1591 as a vulnerability of lesser severity. The latest release of logback, v 1.2.9 released on Dec 21st, 2021 fixes this issue.

Unlike the Log4jShell vulnerability, the logback vulnerability is of a much lower severity level. The Log4jShell vulnerability requires no privilege whereas the logback vulnerability requires significant prior privilege.

eG Enterprise v7 uses earlier versions logback v1.2.3 and hence, by way of this advisory, we are requesting customers who are running eG Enterprise v7 to apply the latest security patches indicated below as soon as possible. It must be noted that since eG agents do not listen on TCP ports for any communications, they are inherently more secure than applications that do listen on TCP ports for inbound requests.

Security Patches for eG Enterprise

We have provided automated patches for eG Enterprise to address the Log4jShell and logback issues.

- To be on the safe side, we have discontinued all usage of log4j in eG Enterprise. This has required changes to the core eG agent, the NetFlow collector, Syslog collector and RUM collector. We have also discontinued use of log4j in the eG manager.

- To address the logback issue, we have changed the eG Enterprise components to use logback v 1.2.9. Logback's configuration file is also being made read-only, as advised in http://slf4j.org/log4shell.html.

These patches are available for the eG Manager v7.1 and eG Agents v7.1 (all OS). Patches for the eG Enterprise RUM collector are also available. You can access these patches using the following URLs:

For v 7.1.8 / v7.1.9:

http://download.eginnovations.com/eval718/Patches/Log4JShell/
OR
https://www.eginnovations.com/eval718
Navigate to the "Patches/Log4JShell" folder.

For the agent patches, please check if you are using v7.1.8 or v7.1.9 for the agents and use the appropriate patch.

For v 7.1.6:

http://download.eginnovations.com/eval716/Patches/Log4JShell/
OR
https://www.eginnovations.com/eval716
Navigate to the "Patches/Log4JShell" folder.

For v 7.1.4:

http://download.eginnovations.com/eval714/Patches/Log4jShell/
OR
https://www.eginnovations.com/eval714
Navigate to the "Patches/Log4JShell" folder.

(Please contact your eG Innovations support team if you do not have access to these URLs).

☞ Note that eG Enterprise v6 has reached end of life. Hence, we are not releasing any patches for customers running eG Enterprise v6.

For customers using eG Enterprise SaaS, please note that our SaaS systems have been updated with these patches already.

Note:

- **If you applied the security patches uploaded on Dec 13/14, 2021, these new patches need to be re-applied again.** Log4j and Logback issued three different patches during the last week and we had to react to these changes.
- eG Enterprise will not use Log4j and logback from the next major release – eG Enterprise v7.2.
- If you are running version 6.x of the eG Manager, you should upgrade as soon as possible to the latest version - eG Manager v7.1.8 and then apply the patch mentioned above.
- The manager patch mentioned above can also be installed on an eG Super Manager.
- eG VM agents and eG SCOM connector do not use Log4j or logback at all.

Instructions for Patch Deployment

Security patches are available for v7.1.8, v7.1.6, and v7.1.4 of eG Enterprise. The procedures outlined below apply, regardless of the version of eG manager/agent/RUM collector in use in your environment.

Instructions for deploying the eG manager patch:

To deploy the eG manager patch, do the following:

- From the eG manager host, access the URL provided above, and click on the **Manager** folder.
- Then, click on the sub-folder that corresponds to the operating system of your eG manager.
- Next, download the zip file within to any folder on the manager host.
- Extract the contents of the downloaded zip to the same folder.
- Go to the folder containing the extracted contents, and run the batch/script file within to upgrade the eG manager.
- Note that the eG manager will be automatically restarted once the patch deployment succeeds.

When running the patch, choose the **A** (Apply) option. Once you have verified that the manager is running well after the patch, you can commit the upgrade by re-running the upgrade batch file/script and entering **C** (Commit) at the prompt.

Instructions for deploying the eG agent patch:

The eG agents are auto-upgradeable. The instructions below can be used to upgrade the eG agent. Note that for agents that serve as NetFlow collectors, the agent patch will not perform any action. We will be providing an additional patch for agents that function as NetFlow collectors in a week's time.

- From the eG manager host, access the URL mentioned above, and click on the **Agent** folder.

- Download the zip files in the OS-specific sub-folders under **Agent** to the corresponding folders of the **<**EG_MANAGER_INSTALL_DIR>\manager\config\tests directory.
- Then, enable the **Auto-upgrade** capability of the eG agents using the Agents -> Upgrade -> Settings menu sequence.
- When the eG agents check the manager for the existence of upgrade patches, they will automatically download the patch files and install them.

If you wish to update the agent on a master image (e.g., VM snapshot, Citrix PVS Gold Image, AWS AMI etc), you can use the files provided in the "*Master_Image_Update*" folder. Download all the files to the master image, in the eG Agent folder and run the "eGupgrade.bat" script.

Instructions for upgrading the eG Java APM library - eg_btm.jar file

The eG Java APM library – eg_btm.jar – which is used for transaction tracing of Java applications uses logback and hence has been modified. You must follow the instructions in this section only if you are using eG Java APM on a system.

Important Note: eG BTM jar should not be replaced when the application server JVM that using this jar file is running.

- Updating the eg_btm.jar while the application JVMs that use it are running is not advisable. So when the agent patch is deployed, the updated eg_btm.jar file is copied as "eg_btm_logback_fixed.jar" in the following directory:
    - Unix : /opt/egurkha/lib/apm/Java/default/
    - Windows : /EGURKHA_HOME/lib/apm/Java/default/

  One or more JVMs running on a system can make use of the same eg_btm.jar. So if all the JVMs refer to the BTM jar file from the above directory, the procedure to upgrade is:

    - Stop the application server JVMs.
    - Take a backup of existing eg_btm.jar that is currently being used.
    - Rename the "eg_btm_logback_fixed.jar" as eg_btm.jar.
    - Start the application server JVMs.

- It is possible that in some deployments, the eg_btm.jar may be copied to a different directory other than default directory and applications may be referring to this file. For such cases, you have to take extra care to replace all instances of eg_btm.jar with the latest eg_btm_logback_fixed.jar file. Deploying the agent patch will not copy the eg_btm.jar file to these non-default directories.

  To update the eg_btm.jar file use the below steps.

    - Stop the application server JVMs.
    - Take a backup of existing eg_btm.jar that is currently being used.
    - Replace the eg_btm.jar with the eg_btm_logback_fixed.jar file.
    - Rename eg_btm_logback_fixed.jar to eg_btm.jar.
    - Start the application server JVMs.

Instructions for deploying the eG RUM Collector patch:

The eG RUM collector which is used to collect real user experience metrics from browser clients also uses log4j v1. If you are not using an eG RUM collector in your infrastructure, you can ignore the instructions below.

- If the RUM collector bundled with the eG manager is used in your infrastructure, no additional patches are needed. The eG manager patch mentioned earlier is sufficient to remove log4j references from the eG RUM collector.
- If you have used the eG RUM Collector installer to set up a dedicated RUM collector (Microsoft Windows OS only), there is a separate automated patch provided in the URL mentioned above (The patch is available in the folder "RumCollector -> Separate RUM Collector"). You can use this patch to update the RUM collector.
- If you have set up a RUM collector using your own application server, deploying the eG RUM collector WAR distribution on it, there are automated patches provided for Windows and Linux OS (The patches are available in the folder "RumCollector -> RUM Collector WAR").

If you have any questions regarding this note, or would like any assistance with updating the patches, please contact your eG Innovations support team asap.

Change Log:

- First released on Dec 13, 2021.
- Instructions for installing the manager patches have been provided.
- Instructions for patching the eG RUM collector have been added.
- Dec 14: Agent patches updated with instructions.
- Dec 22: Added details of logback vulnerability and work around.