NetIQ Release Notes

NetIQ Access Manager Patch Release for Log4j Vulnerability

December 2021

This patch release includes a fix for CVE-2021-44228 and CVE-2021-45046 vulnerabilities. This patch is supported for the following versions of the product:

- Access Manager 5.0
- Access Manager 5.0 Service Pack 1
- Access Manager Appliance 5.0 Service Pack 1

IMPORTANT: For Access Manager 5.0 Service Pack 1 container deployment, you need to refresh the docker images. See "Applying the Vulnerability Fix on Containers" on page 3.

In this Article

Security Vulnerability Fixes

This release fixes the following Log4J vulnerability issues:

- CVE-2021-44228 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228)
- CVE-2021-45046 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046)

Applying the Patch

IMPORTANT: In a cluster setup, ensure that you install the patch on each node of the Access Manager setup.

- "Downloading the Patch" on page 2
- "Installing the Patch" on page 2

Downloading the Patch

Download the patch file from the Software License and Download portal.

Table 1 *Files Available for Access Manager Patch Release for the Log4J Vulnerability:*

Filename	Description
`AM_log4j_Patch_Linux64.tar.gz`	Contains the Log4j vulnerability fix for Access Manager (Administration Console, Identity Server, Access Gateway) on Linux and Access Manager Appliance.
`AM_log4j_AnalyticsServer_Patch.tar.gz`	Contains the Log4j vulnerability fix for Analytics Server.
`AM_log4j_Containers.tar.gz`	Contains Administration Console, Identity Server, Access Gateway, and Analytics Server images with Log4j vulnerability fix. Use it if you do not want to download images from the public docker hub. This file also contains the eDirectory image. However, this image does not have any fix as it does not contain Log4j libraries.

Installing the Patch

- Access Manager on Linux and Access Manager Appliance
- Analytics Server

IMPORTANT:

- During installation of the patch, all running services are stopped temporarily. After the patch is installed, all services are restarted.
- After installing this patch, the version number of Access Manager components is not changed.

Access Manager on Linux and Access Manager Appliance

1. Extract the patch file by using the `tar xvf AM_log4j_Patch_Linux64.tar.gz` command.
2. Go to the location where you have extracted the patch files.
3. Run the `install_patch.sh` script in the extracted `AM_log4j_Patch_Linux64` folder as a root or root equivalent user.
4. To validate whether the patch is applied successfully, run the following command and check the jar versions are 2.16.0:

   ```
   find / -name log4j-core*.jar
   ```

Analytics Server

1. Extract the patch file by using the `tar xvf AM_log4j_AnalyticsServer_Patch.tar.gz` command.
2. Go to the location where you have extracted the patch files.
3. Run the `ar_install_patch.sh` script in the extracted `AM_log4j_AnalyticsServer_Patch` folder as a root or root equivalent user.

4. To validate whether the patch is applied successfully, run the following command:

   ```
   find / -name log4j*.jar | xargs grep org/apache/logging/log4j/core/lookup/
   JndiLookup.class
   ```

NOTE: You might see log4j-core-2.16.0.jar in /opt/novell/devman/jcc/lib/. Ignore that as it is not vulnerable.

Applying the Vulnerability Fix on Containers

If the version of your Access Manager or Analytics Server is 5.0, you must upgrade these to 5.0 Service Pack 1 to fix the Log4j vulnerability. If you are already on 5.0 Service Pack 1, pull the latest version of 5.0 Service Pack 1 images.

The steps to apply the vulnerability fix are the same in both of the following scenarios:

- **Upgrading from 5.0 to 5.0 Service Pack 1:** Ensure that you have the Helm chart of 5.0 Service Pack 1. You can download the chart from the Software License and Download portal. For more information, see NetIQ Access Manager 5.0 Service Pack 1 Release Notes.
- **Upgrading images from 5.0 Service Pack 1 to the latest 5.0 Service Pack 1:** Follow the steps in the proceeding section and update `values.yaml` of the access-manager-1.0.1 chart, which was used in the 5.0 Service Pack 1 deployment. If you do not have that chart folder, download the 5.0 Service Pack 1 chart again. Ensure to retain your existing deployment values.

  The steps will pull only the latest images of 5.0 Service Pack 1, and the version of the product will not be changed.

NOTE: If you do not want to download the images from the public docker hub, download `AM_log4j_Containers.tar.gz` from the Software License and Download portal. This file contains the latest 5.0 Service Pack 1 images with Log4j vulnerability fix for the following components:

- Administration Console
- Identity Server
- Access Gateway
- Analytics Server

This file also contains the eDirectory image. However, this image does not have any fix as it does not contain Log4j libraries.

This section includes the following information:

- Applying the Vulnerability Fix on Access Manager Container
- Applying the Vulnerability Fix on Analytics Server Containers

Applying the Vulnerability Fix on Access Manager Container

You can pull the latest images with vulnerability fixed by performing the following steps:

1. Run the following command to view all releases and their namesapces:

   ```
   helm list -A
   ```

   Choose the access-manager release and the namespace.
2. In the extracted chart folder, update the values in access-manager-1.0.1/values.yaml as follows:

NOTE: For Access Manager 5.0, download access-manager-1.0.1 charts and update all values from access-manager-1.0.0/values.yaml to access-manager-1.0.1/values.yaml.

```
image:
pullPolicy: Always

am-ac:
primary:
mode: upgrade

secondary:
mode: upgrade
```

NOTE: Ensure that you reuse the values that were used in your earlier deployment or reuse the same `values.yaml` file.

3 Run the following helm upgrade command:

```
helm upgrade <release-name> <name-of-the-helm-chart> -n <name-of-the-namespace>
```

For example:

If the current deployment is 5.0 Service Pack 1: `helm upgrade nam access-manager-1.0.1 -n development`

If the current deployment is 5.0: `helm upgrade nam access-manager-1.0.0 -n development`

NOTE: For Access Manager 5.0 Service Pack 1, these steps will pull the latest images of the same version and the version number will not be changed.

4 To validate that the old Log4j libraries are updated with the latest Log4j libraries (version 2.16), perform the following steps:

4a Run the following command to list pods details for Access Manager:

kubectl get pods -n < namespace > | grep < release name >

Identify the required pods.

4b Run the following commands on Administration Console, Identity Server, and Access Gateway pods:

```
kubectl exec <Administration Console/Identity Server/Access Gateway pod name> -c <Administration Console/Identity Server/Access Gateway container name> -n <namespace> -- find . / -name log4j*.jar -ls
```

Examples:

Administration Console: `sudo kubectl exec nam-am-ac-0 -c am-ac -n development -- find . / -name log4j*.jar -ls`

Identity Server: `sudo kubectl exec nam-am-idp-0 -c am-idp -n development -- find . / -name log4j*.jar -ls`

Access Gateway: `sudo kubectl exec nam-am-ag-0 -c am-ag -n development -- find . / -name log4j*.jar -ls`

NOTE: You might see a few instances of very old versions of Log4j libraries, such as log4j-1.2.15.jar or log4j-1.2.14.jar. Ignore these lower version libraries as these are not vulnerable.

Applying the Vulnerability Fix on Analytics Server Containers

You can pull the latest images with vulnerability fixed by performing the following steps:

1. Run the following command to view all releases and their namesapces:

   ```
   helm list -A
   ```

   Choose the dashboard release name and the namespace.

2. In am-dashboard-1.0.1/values.yaml, update `pullPolicy` to `Always`.

   NOTE: For Analytics Server 5.0, download am-dashboard-1.0.1 charts and update all values from am-dashboard-1.0.0/values.yaml to am-dashboard-1.0.1/values.yaml.

   ---

3. Run the following helm upgrade command:

   If the current deployment is 5.0 Service Pack 1: `helm upgrade <dashboard-release-name> am-dashboard-1.0.1 -n <namespace-of-release>`

   If the current deployment is 5.0: `helm upgrade <dashboard-release-name> am-dashboard-1.0.0 -n <namespace-of-release>`

   NOTE: For Analytics Server 5.0 Service Pack 1, these steps will pull the latest images of the same version and the version number will not be changed.

   ---

4. To validate that the old Log4j libraries are updated with the latest Log4j libraries (version 2.16), perform the following steps:

   4a Run the following command to list pods details for the dashboard:

   ```
   kubectl get pods -n < namespace > | grep < dashboard release name >
   ```

   Identify the required pod.

   4b Run the following command on the dashboard container to go into the pod:

   ```
   kubectl exec it <dashboard_pod_name> -n <namespace> /bin/bash
   ```

   For example: `kubectl exec -it am-dashboard-0 -n automation /bin/bash`

   4c Run the following command in the pod:

   ```
   find / -name log4j*.jar | xargs grep org/apache/logging/log4j/core/lookup/
   JndiLookup.class
   ```

   NOTE: You might see log4j-core-2.16.0.jar in /opt/novell/devman/jcc/lib/. Ignore that as it is not vulnerable.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://www.microfocus.com/support-and-services/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- The Micro Focus Community pages: https://www.microfocus.com/communities/

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/about/legal/.