Advanced Authentication 6.3 Service Pack 6 Patch 1 Release Notes

December 2021

Advanced Authentication 6.3 Service Pack 6 Patch 1 resolves CVE-2021-44228 and CVE-2021-45046 vulnerabilities.

If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of the specific page in the HTML version of the documentation posted at the NetIQ Advanced Authentication Documentation page.

Security Vulnerability Fixes

This release mitigates the following security issues:

- Apache Log4j Remote Code Execution Vulnerability. (CVE-2021-44228)
- Apache Log4j 2.15.0 (the fix to address CVE-2021-44228) was discovered to create malicious input data using a JNDI Lookup pattern and causing a denial of service (DOS) attack. (CVE-2021-45046)

NOTE: Some Security tools might indicate that mitigations are not appropriate. To manually validate the mitigations, perform the following in the Linux console on each server in the cluster (as the root user):

1. Run the following command:

   ```
   docker exec aaf_searchd_1 bash -c 'ps -efww | grep java'
   ```

   Several variables are displayed, check the JNDI lookups system property is set to True in the Global Master server. This indicates that the JNDI lookups is disabled.

   ```
   -Dlog4j2.formatMsgNoLookups=true
   ```

NOTE: This setting is available on the Global Master servers. It does not apply to other Advanced Authentication servers because elastic search is only active on Global Master servers.

2. Run the following commands:

   ```
   docker exec -it aaf_searchd_1 bash
   ```

   ```
   unzip lib/log4j-core-*.jar org/apache/logging/log4j/core/lookup/
   JndiLookup.class
   ```

   The following message is displayed to indicate that the `JNdiLookup.class` has been removed from the class path:

   ```
   caution: filename not matched: org/apache/logging/log4j/core/lookup/JndiLookup
   ```

Upgrading

You can upgrade to Advanced Authentication 6.3 Service Pack 6 Patch 1 from one of the following versions of Advanced Authentication:

- 6.3
- 6.3.1
- 6.3.2
- 6.3.3
- 6.3.4
- 6.3.5
- 6.3.6

For more information about upgrading, see "Upgrading Advanced Authentication" in the *Advanced Authentication- Server Installation and Upgrade* guide.

Planned End of Support in Advanced Authentication 6.4

- The options, **Push salt TTL** and **Authentication salt TTL** will be removed from the **Smartphone** method settings.
- The user credentials prompt for HTTPS proxy will be removed during login and the credentials will be made available in the `config` file.

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notice