Addressing the Java Deserialization Vulnerability for SAS Software

Note: *If you have applied SAS Security Update 2015-1 or 2016-02 and the hot fixes associated with them, you should still apply SAS Security Update 2016-06 and its associated hot fixes. SAS Security Update 2016-06 and its associated hot fixes address additional fixes for this Java vulnerability.*

If you downloaded a SAS 9.4_M3 order after October 18, 2016 or any SAS 9.4_M4 order, the fixes in SAS Security Update 2016-06 are included in your order. The SAS Deployment Wizard will install SAS Security Update 2016-06 during your software deployment or update. You can skip sections 1-3 in this document, but you should still perform the steps in section 4.

This document describes the steps you should take in order to apply SAS Security Update 2016-02 and the hot fixes associated with it. It is critical that the steps be performed in the order they appear in this document. It is also critical that you perform all of the steps the first time that you apply the update and hot fixes.

These steps may direct you to apply a hot fix you have already applied outside this process. If so, follow the instructions and re-apply the hot fix. The SAS Deployment Manager will determine if any hot fix has been previously applied and tell you what hot fixes it did apply. If it finds that a hot fix has been previously applied, you do not have to perform any of the post-installation steps for that hot fix.

Note: *If your deployment is an upgrade, the Y09004 hotfix and SAS Security Update must be applied, in any order, between the install and configuration steps.*

Section 1 — Apply SAS Security Update 2016-06

Note: *To determine if you have already applied this version of the SAS security update, locate and examine the contents of these files:*

```
SASHome\InstallMisc\utilities\installqual\9.4\serialization_hotfi
x.properties
```

```
SASHome\instqualtool\serialization_hotfix.properties
```

If the file does not exist in either location or it lists the version of the SAS security update as less than 3.0, you do not have this latest version of the update.

Note: *If your middle tier is horizontally clustered, complete Sections 1-4 on the primary middle tier machine or machines first and then complete Section 5 for the secondary middle tier cluster nodes.*

Use the following steps to apply the security update. These instructions should be followed for every machine in your deployment (except the secondary middle tier cluster nodes which will return you to

this section after some preliminary steps are completed), either by putting the update individually on each machine or running the update from a networked location that each machine has access to.

1. Before beginning, ensure all active SAS sessions, daemons, spawners, servers, and agents are terminated. In addition, SAS strongly recommends that you back up your system before applying the hot fix.

2. Download the security update from
   http://ftp.sas.com/techsup/download/hotfix/HF2/Java-deserialization_update.html#update

3. Unzip `sas-security-update-2016-06.zip` into a directory of your choice. On UNIX, using `unzip` is the best option, but if you use WinZip or the `jar xvf` command, you must also use the following command in order to preserve the appropriate permissions:

   ```
   chmod a+x install.sh
   ```

   If the install ID differs from the security update directory owner, make the directory writable by all IDs in the same group with the following command:

   ```
   chmod -R g+w /<security directory>/sas-security-update-2016-06
   ```

4. From the directory into which you've unpacked the software, go to the `sas-security-update-2016-06` directory.

5. In that directory, run the appropriate script using the same user ID that was used to install the software. The script requires one argument, the full path to the SASHOME where the hot fix is going to be applied.

   Windows

   ```
   install.bat "<SASHOME>"
   ```

   Windows Example

   ```
   install.bat "C:\Program Files\SASHome"
   ```

   *Note: Depending on your settings, you may have to use the **Run as administrator** option.*

   UNIX

   ```
   ./install.sh "<SASHOME>"
   ```

   UNIX Example

   ```
   ./install.sh "/usr/lpp/SAS"
   ```

6. The tool runs and applies the hot fix to all the files in the SASHOME and SASConfig that need to be updated. When the tool finishes making the updates, it provides a message that says the updates are complete and then exits.

7. If you plan to deploy other hot fixes from the location where you placed this zip file, you will need to remove it from this location. The SAS Deployment Manager, which is used for deploying other hot fixes, will not recognize this file and will issue an error.

Section 2 — Apply Hot Fix Y09004 - Supplemental Hot Fix for SAS Security Update 2016-06

Hot fix Y09004 is a container hot fix that contains fixes for several products. Your deployment may not contain all of the products included in this hot fix container: the tools will skip updates if they do not apply to your deployment. We have packaged these together to make the update simpler.

Ensure that all active SAS sessions, daemons, spawners, servers, and agents remain terminated. Then follow these instructions to apply hot fix Y09004.

1. Go to http://ftp.sas.com/techsup/download/hotfix/HF2/Java-deserialization_update.html#Y09004

2. Use the instructions in the Y09004pt.pdf file at that location to apply hot fix Y09004 to every machine, except secondary middle tier cluster machines, in your deployment.

Section 3 — Rebuild and Redeploy Web Applications

After the update and hot fixes have been applied, you must rebuild and redeploy every web application on each middle tier machine in order to assure the hot fixes can take effect. The instructions for rebuilding and redeploying can be found in the following locations:

Rebuilding - refer to the "Rebuilding the SAS Web Applications" topic in the "Administering SAS Web Applications" section of the "Middle-Tier Applications" chapter of the *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide* located at http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html

Redeploying - refer to the "Redeploying the SAS Web Applications" topic in the "Administering SAS Web Applications" section of the "Middle-Tier Applications" chapter of the *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide* located at http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html

Section 4 — Product-Specific Hot Fixes

Apply product-specific hot fixes using the following steps.

1. Go to http://ftp.sas.com/techsup/download/hotfix/HF2/Java-deserialization_update.html#prodhotfix to review a list of product-specific Java Deserialization hot fixes.

2. Click on the links for the hot fixes, if any, that apply to your deployment.

3. Read the documentation about applying the hot fixes you will apply.

4. Optionally, run the HFADD tool to generate a report of other hot fixes that you may want to apply to your deployment.

   Note: *If you use the HFADD tool, SAS Security Update 2016-06 and hot fix Y09004 will never be included in the results. SAS Security Update 2016-06 and hot fix Y09004 must always be applied manually according to the instructions above.*

5. Once you have determined all the hot fixes to apply to your deployment, download them and place them in a directory on each machine or in a shared location each machine can access per the instructions provided in the *SAS Deployment Wizard and SAS Deployment Manager 9.4: User's Guide*.

6. Perform any pre-installation tasks in the documentation that accompanies each hot fix.

7. Apply the hot fixes.

8. Perform any post-installation tasks in the documentation that accompanies each hot fix.

Section 5 — Apply the Java Deserialization Fix to a Horizontal Middle-Tier Cluster Node

For information about applying the Java Deserialization Fix to a horizontal middle-tier cluster, see SAS Note 59810 at http://support.sas.com/kb/59/810.html

Product-specific hot fixes may require additional manual steps for configuration on   horizontal middle-tier cluster nodes. Please review the individual hot fix installation documentation for additional steps required.

Contacting SAS Technical Support

If you need assistance with the software, we ask that only SAS support personnel call our Technical Support Division.

- For U.S. and Canadian customers, support is provided from our corporate headquarters in Cary, North Carolina. You may call (919) 677-8008, Monday through Friday.
- Customers outside of the U.S. can obtain local-language technical support through the local office in their countries. Customers in these locations should contact their local office for specific support hours. See http://support.sas.com/techsup/contact/index.html for contact information for local offices.

20 April 2017