

Addressing the Java Deserialization Vulnerability for SAS Software

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.

Note: *If you have applied SAS Security Update 2015-11 and the hot fixes associated with it, you should still apply SAS Security Update 2016-02 and its associated hot fixes. SAS Security Update 2016-02 and its associated hot fixes address additional fixes for this Java vulnerability..*

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 in place, the Y09002 hotfix and SAS Security Update must be applied, in any order, between the install and configuration steps. This direction can be ignored if the upgrade in place is from a SAS 9.4_M3 order for Ship Event 16w17 or later (after April 28, 2016).*

After the update and the hot fixes described in this document have been applied, if you subsequently update your deployment with additional products or other hot fixes, you should repeat step 1 and step 3 below to ensure continuous security.

Step 1 — Apply SAS Security Update 2016-02

Note: *If you downloaded a SAS 9.4_M3 order for Ship Event 16w17 or later (after April 19, 2016), the fixes in SAS Security Update 2016-02 are included in your order. You do not need to perform this step.*

Use the following steps to apply the security update. These instructions should be followed for every machine in your deployment, whether it is 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-2016-02.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
```
4. From the directory into which you've unpacked the software, go to the `sas-security-update-2016-02` 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.

After the tool exits, the zip file should be either moved to another location or deleted because its presence will prevent successfully applying subsequent hot fixes that are stored in the same location.

Step 2 — Apply Hot Fix Y09002 - Supplemental Hot Fix for SAS Security Update 2016-02

Note: If you downloaded a SAS 9.4_M3 order for Ship Event 16w17 or later (after April 28, 2016), the fixes in hot fix Y09002 are included in your order. You do not need to perform this step.

Hot fix Y09002 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 Y09002.

1. Go to http://ftp.sas.com/techsup/download/hotfix/HF2/Java-deserialization_update.html#Y09002
2. Use the `Y09002pt.pdf` file at that location to apply hot fix Y09002. Hot fix Y09002 should be applied to every machine in your deployment, per the instructions.

Step 3 — Rebuild and Redeploy Web Applications

Note: If you downloaded a SAS 9.4_M3 order for Ship Event 16w17 or later (after April 28, 2016), you should not have performed either step 1 or 2. You do not need to perform this step.

After the update and hot fixes have been applied, you must rebuild and redeploy every web application in order that 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>

If you have middle-tier clusters, run the SAS Deployment Wizard on the middle-tier cluster nodes and configure in order to “synch” the cluster nodes with the primary.

Step 4 — Apply Hot Fix for SAS Web Server and SAS Environment Manager

The specific hot fix that is required for the SAS Web Server is determined by the version of SAS that you are using. Consult the following table to determine the hot fix that you should download and apply.

SAS Version	Hot Fix to Apply	Hot Fix Location
SAS 9.4 M3	V770xx	http://ftp.sas.com/techsup/download/hotfix/HF2/Java-deserialization_update.html#V770xx
SAS 9.4 M2	S470xx	http://ftp.sas.com/techsup/download/hotfix/HF2/Java-deserialization_update.html#S470xx
SAS 9.4 M1	S480xx	http://ftp.sas.com/techsup/download/hotfix/HF2/Java-deserialization_update.html#S480xx
SAS 9.4 M0	S460xx	http://ftp.sas.com/techsup/download/hotfix/HF2/Java-deserialization_update.html#S460xx

The listed hot fixes are container hot fixes that apply updates to the SAS Web Server and to SAS Environment Manager.

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

1. Go to the location, listed in the **Hot Fix Location** column in the table above, for the version of SAS that you are using.

2. At that location, follow the instructions in the html file that is appropriate for your operating system in order to apply the hot fix and perform any post-installation tasks that are required. The hot fix should be applied to every machine in your deployment, per the instructions. The instructions will direct you to the *SAS Deployment Wizard and SAS Deployment Manager 9.4: User's Guide*, which in turn will tell you to use the HFADD tool. Using HFADD may add other hot fixes than the ones listed in this document. Those additional hot fixes should also be applied in order to have the latest fixes for all your products.

Note: *When you use the HFADD tool, SAS Security Update 2016-02 and hot fix Y09002 will never be included in the results. SAS Security Update 2016-02 and hot fix Y09002 must always be applied manually according to the instructions above.*

When you have finished the post-installation tasks for the SAS Web Server hot fix, the updates to address the Java deserialization vulnerability are complete.

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.