Access Manager 4.0 Hotfix 2 Readme

April 2014

The Access Manager 4.0 Hotfix 2 supercedes Access Manager 4.0 Hotfix 1 and includes an important security fix to resolve the Heartbleed vulnerability being tracked by OpenSSL bug CVE-2014-0160. For more information about this vulnerability, see US-Cert Technical Alert.

If you are on Access Manager 4.0, you are not affected by the Heartbleed vulnerability. But if you are on Access Manager 4.0 Hotfix 1 and have installed the additional package to enable Transport Layer Security (TLS) version 1.1 and 1.2, there is a security vulnerability in the version of OpenSSL library that is used by the additional package.

1 What’s New in Access Manager Hotfix 2?

This hotfix includes an important fix to resolve the Heartbleed bug in OpenSSL and also includes all the software fixes in Access Manager Hotfix 1.

For the list of software fixes, enhancements and known Issues in the Access Manager 4.0 and Access Manager 4.0 Hotfix 1 releases, see Access Manager 4.0 Readme and the Access Manager 4.0 Hotfix 1 Readme.

2 Determining If You Are Affected By This Vulnerability

The Identity Server and Administration Console do not use OpenSSL and are therefore not affected by the Heartbleed vulnerability.

The Access Gateway uses OpenSSL to provide support for secure communication. The Access Gateway in Access Manager 4.0 uses OpenSSL 0.9.8 and is therefore not affected by the Heartbleed vulnerability. If you are on Access Manager 4.0 Hotfix 1 and have installed the additional package to enable Transport Layer Security (TLS) version 1.1 and 1.2, there is a security vulnerability in the version of OpenSSL library that is used by the additional package

To determine if the Access Gateway is susceptible to the Heartbleed vulnerability, execute the following steps on all Access Gateway 4.0 HF1 servers:

1. Open a terminal window and run the following command to determine the version of OpenSSL:

   ```
   rpm -qa|grep nacm
   ```

2. If the package list displayed includes the `novell-nacm-apache-openssl101f-2.2.24-400110` package, then the system is affected by the Heartbleed vulnerability. Therefore it is mandatory to upgrade to Access Manager 4.0 Hotfix 2. For more information about upgrading, see Upgrading

to Hotfix 2.

If the output of the command does not display the `novell-nacm-apache-openssl101f-2.2.24-400110` package, then the system is not affected by the Heartbleed vulnerability. It is still recommended that you upgrade to Hotfix 2 as it includes software fixes introduced in Hotfix 1.

3 Upgrading to Hotfix 2

NOTE: Ensure that you are currently on Access Manager 4.0 or Access Manager 4.0 Hotfix 1 before upgrading to Access Manager Hotfix 2.

To upgrade to Access Manager 4.0 Hotfix 2, download the `AM_400_HF2.zip` file that contains the Access Manager Patch Tool and the patch file using the following steps:

1. Go to NetIQ downloads page.
2. Under **Patches**, click **Search Patches**.
3. Specify `AM_400_HF2.zip` in the search box and download the Hotfix file.
4. Upgrade using the procedure described in Upgrading Access Manager Using the Patch Process for Linux and Upgrading Access Manager 4.0 Using the Patch Process for Windows.
5. On the Access Gateway server, if the output of the `rpm -qa|grep nacm` command includes the `novell-nacm-apache-openssl101f-2.2.24-400110` package, then it is important to reinstall the Access Gateway packages to enable TLS 1.1 and TLS 1.2. For more information about this, see Section 2 in Enabling TLS 1.1 and TLS 1.2 for Access Manager 4.0 Hotfix 2.

3.1 Verifying Version Numbers Before Upgrading

You can upgrade to Access Manager 4.0 Hotfix 2 if you are on Access Manager 4.0 or Access Manager 4.0 Hotfix 1.

Before upgrading, it is important to verify the version number of the existing Access Manager components. This ensures that you have the correct version of files on your system.

3.1.1 Verifying Version Number if you Are on Access Manager 4.0

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**.
2. Examine the value of the **Version** field to see if it displays version 4.0.0-110.

3.1.2 Verifying Version Number if You Are on Access Manager 4.0 HotFix 1

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**.
2. Examine the value of the **Version** field to see if it displays version 4.0.0-110 + HF1-139.

3.2 Verifying Version Numbers After Upgrading

After upgrading to Access Manager 4.0 Hotfix 2, verify the version number of the components using the following procedure:

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**
2. If you upgraded from Access Manager 4.0, verify that the **Version** field to see if it displays version 4.0.0-110 + HF2-141.
3. If you upgraded from Access Manager 4.0 Hotfix 1 to Hotfix 2, verify that the **Version** field displays version 4.0.0-110 + HF1-139, HF2-141.

4 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 Web site.

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

You can post feedback in the Access Manager forum on Qmunity (http://community.netiq.com/forums/30.aspx), our community Web site that also includes product notifications, blogs, and product user groups.

To download this product, go to Access Manager on the All Products Page (http://www.netiq.com/products).

5 Legal Notice

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see http://www.netiq.com/company/legal/.

[Return to Top]