Access Manager Appliance 4.0 Service Pack 1 Hotfix 3 Release Notes

December 2014

![(Product Name and Version)] The Access Manager Appliance 4.0 Service Pack 1 Hotfix 3 (4.0.1 HF3) supercedes Access Manager Appliance 4.0 Service Pack 1 Hotfix 2.

For the list of software fixes and enhancements in the previous release, see Access Manager Appliance 4.0 SP1 HF1 readme.

1 What’s New?

This release includes the platform updates and fixed issues.

1.1 Platform Updates

This release includes the following platform updates:

- eDirectory 8.8 SP8_FTP4
- iManager 2.7.7.3
- Java 1.7.0.72
- OpenSSL 101J

1.2 Fixed Issues

The following fixed issues are included in this release:

1.2.1 Software Fixes for the Administration Console

The following issues are fixed in the Administration Console:

1.2.1.1 Cross-Site Scripting Vulnerability Issue in JSP Files

Issue: In the Administration Console, multiple cross-site vulnerabilities exist in `.jsp` files. [Bug 906241]

Fix: This issue is resolved by sanitizing the `.jsp` files.

1.2.1.2 JSP Files Display Sensitive Information to an Authenticated Administrator

Issue: In the Administration Console, the administrator can view internal credential details using specific .jsp files.. [Bug 904677]

Fix: This issue is resolved by decrypting the credential information and the details are not displayed to the administrator.

1.2.1.3 Wget Utility Vulnerability Issue

Issue: The Wget vulnerability issue allows file systems to be overwritten (CVE-2014-4877) [Bug 903324]

Fix: This release fixes issues with Wget file retrieval utility and the file systems are not overwritten.

1.2.1.4 Cross Site Scripting Issue Injects Script

Issue: Due to cross-site scripting issues, stored script is injected on the Auditing page. [Bug 904689]

Fix: This release fixes the issue by sanitizing the URL.

1.2.2 Software Fixes for the Identity Server

The following issues are fixed in the Identity Server:

1.2.2.1 Cross-Site Scripting Vulnerability Issue in the JSP Page

Issue: In the Identity Server, multiple reflected cross-site scripting vulnerabilities exist in .jsp files. [Bug 904675]

Fix: This issue is resolved by sanitizing the .jsp files

1.2.2.2 Cross-Site Scripting Vulnerability Issue With WS-Federation Authentication Process

Issue: The WS-Federation authentication process is affected by cross-site scripting vulnerabilities. [Bug 903062]

Fix: This issue is resolved by sanitizing the .jsp files.

1.2.3 Software Fixes for the Access Gateway

The following issues are fixed in the Access Gateway:

1.2.3.1 JCC Port 1443 Accepts SSLV3 Requests

Issue: In the Access Gateway, the JCC port 1443 is affected by Poodle vulnerability as it accepts SSLv3 requests. (CVE-2014-3566) [Bug 903876]

Fix: This release fixes the Poodle vulnerability by disabling SSLv3 requests on JCC port 1443.

2 Upgrading to 4.0.1 HF3

IMPORTANT: Ensure that you are currently on Access Manager 4.0 Service Pack 1, 4.0.1 HF1 or 4.0.1 HF2 before upgrading to Access Manager 4.0.1 HF3.

To upgrade Access Manager Appliance 4.0.1 HF3, use the following steps to download the `AM_401_HF3.zip` file that contains the Access Manager Appliance Patch Tool and the patch file:

1. Go to NetIQ downloads page.
2. Under **Patches**, click **Search Patches**.
3. Specify `AM_401_HF3.zip` in the search box and download the file.
4. Upgrade by using the procedure described in Upgrading Access Manager Appliance 4.0 HF* Using the Patch Process in the NetIQ Access Manager Appliance 4.0 SP1 Installation Guide.

3 Verifying Version Numbers

To ensure that you have the correct version of files before you upgrade to Access Manager 4.0.1 HF3, verify the version of existing Access Manager installation.

Before Upgrading:

To verify the version numbers before upgrading to 4.0.1 HF3:

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**
2. Verify that the **Version** field displays the following version.

Components	4.0.1	4.0.1 HF1
All Access Manager Components	4.0.1.88	4.0.1.88 + HF1-93

After Upgrading:

To verify the version number after upgrading to 4.0.1 HF3:

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**
2. Verify that the **Version** field displays the following version:

Components	Upgrading from 4.0.1	Upgrading from 4.0.1 HF1
All Access Manager Components	4.0.1.88 + HF2 -107	4.0.1-88 + HF1-93, HF2-107

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

[Return to Top]