Access Manager Appliance 4.1 Service Pack 2 Hotfix 1 Release Notes

August 2016

![(Product Name and Version)] The Access Manager Appliance 4.1 Service Pack 2 Hotfix 1 (4.1.2 HF1) supersedes Access Manager Appliance 4.1 Service Pack 2

For the list of software fixes and enhancements in the previous release, see .Access Manager Appliance 4.1 SP2 release notes.

1 What’s New?

This release includes the following platform updates and fixed issues:

1.1 Updates for Dependent Components

This release adds support for the following dependent components:

- eDirectory 8.8.8.6
- Java 1.8.0_66
- Apache 2.2.27
- OpenSSL 1.0.1p (The latest OpenSSL updates are available through channel updates.)
- Tomcat 8.0.24
- iManager 2.7.7.5

NOTE: Access Manager 4.1.2 HF1 by default supports Tomcat 8.0.24 and OpenSSL 1.0.1p, but Administration Console uses Tomcat version 7.0.56 due to dependency on iManager.

1.2 Fixed Issues

This release includes software fixes for the following:

1.2.1 Administration Console

The following issues are fixed in Administration Console:

- The Webshell files uploaded through JSP Pages with Cert server Snapins, can trigger system calls. (TID 7017807)
- The .htaccess file from iManager configuration is susceptible to attacks. (TID 7017811)
- The Nessus scan reports in a web application are susceptible to the Clickjacking in iManager. (TID 7017812)
- iManager application URLs are susceptible to the Cross-Site Scripting (XSS) attack. (TID 7017813)
- Access Manager is prone to phishing attack through iFrame manipulation on the Administration Console login page. (TID 7017818)
- Cross-Site Request Forgery prevention is not working under heavy load. (TID 7017817)

1.2.2 Identity Server

The following issues are fixed in Identity Server:

- The risk servlet points to remotely accessible DTD and executes an XML External Entity (XXE) attack. (TID 7017797)
- Identity Server can execute an XXE that can in turn read the any readable file on the system. (TID 7017806)
- Manipulating the Assertion Consumer Service URL in SAML request leads to the XSS vulnerability. (TID 7017808)
- The unsigned request does not validate incoming AuthnRequest Assertion Consumer Service (ACS) URL tag. (TID 7017809)
- Section 1.2.2.1, “The Unsigned Request does not Validate Incoming AuthnRequest Assertion Consumer Service (ACS) URL Tag,” on page 2

1.2.2.1 The Unsigned Request does not Validate Incoming AuthnRequest Assertion Consumer Service (ACS) URL Tag

Issue: When an authentication request from a service provider is not signed, Identity Provider cannot validate the authenticity and integrity of the request. So any malicious user who can intercept the request can change the ACS URL in the request and make the Identity Provider to send the assertion to malicious sites. [`Bug 991660`]

Fix: This issue is resolved. Two SAML options `SAML2_ACS_DOMAIN_WHITELIST` and `SAML2_ACS_URL_RESTRICT` are introduced.

SAML2_ACS_URL_RESTRICT: This option ensures that Identity Provider validates the Assertion Consumer Service URL in the request against the trusted metadata URL before sending the assertion.

To define this option, go to **Devices > Identity Servers > IdP Cluster > SAML2 >** *[Service Providers*] **> Options > New > OTHERS**. Specify **Property Value** as **True**

SAML2_ACS_DOMAIN_WHITELIST: This option ensures that Identity Provider validates the Assertion Consumer Service URL in the request against a white list of domains.

To define this option, go to **Devices > Identity Servers > IdP Cluster > SAML2 >** *[Service Providers*] **> Options > New > OTHERS**. Specify **Property Value** as domain names separated with semi-colon(;) and no space. For example, *www.airlines.com*;*www.example.com*.

2 Upgrading to 4.1.2 HF1

IMPORTANT: Ensure that you are currently on Access Manager 4.1.2 before upgrading to Access Manager 4.1.2 HF1.

To upgrade Access Manager Appliance 4.1.2 HF1, perform the following steps:

1. Go to NetIQ Downloads Page.
2. Under **Patches**, click **Search Patches**.
3. Specify `AM_4121.zip` in the search box and download the file.
4. Save the hotfix file to the server running Access Manager. If you have multiple servers in your set up, ensure that you copy this .zip file to all the servers.
5. Extract the patch file by using the unzip `<patch name>` .zip command, where <patch filename> is the name of the patch file, for example, `AM_4121.zip`. For more information about the upgrade process, see Upgrading to Access Manager Appliance 4.1.2 Hotfix 1 Using the Patch Process in the NetIQ Access Manager Appliance 4.1 Installation and Upgrade Guide.
6. Run the `sh installPatch.sh` command. This command installs the patch and the bundled binaries.

3 Verifying Version Numbers

To ensure that you have the correct version of files before you upgrade to Access Manager 4.1.2 HF1, verify the existing Access Manager version.

3.1 Verifying Version Number Before and After Upgrading to 4.1.2 HF1

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.

After upgrading to Access Manager 4.1.2 HF1, verify that the version number of the component is indicated as **4.1.2.1-5** in the **Version** field.

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, 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.

5 Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.