Access Manager Appliance 3.2 Service Pack 3 HF1 Readme

January 2015

Access Manager Appliance 3.2 Service Pack 3 HF1 resolves several previous issues.

For the list of software fixes in the previous release, see Access Manager Appliance 3.2 SP3 readme.

IMPORTANT: To upgrade to 4.0 SP1 from 3.2 SP3 HF1, perform the following steps:

1. On the 3.2.3 HF1 server, unzip the 4.0 SP1 executables using `tar-xzvf <file name>` command. For example, to unzip the Access Gateway file, use `tar -xzvf novell-access-gateway-4.0.1-88.tar.gz` command.
2. Replace the `upgrade_utility_functions.sh` file in the 4.0 SP1 executables folder (*extracted_folder*/scripts) with the `/opt/novell/nam/update/HF1/401UpgradeSupport/scripts/upgrade_utility_functions.sh` file.
3. On the 3.2.3 HF1 server, upgrade the components using the information in Upgrading Access Manager.

1 What’s New?

This release includes the following platform updates and fixed issues:

1.1 Updates for Dependent Components

In this release, the following dependent components are updated to fix the vulnerability issues:

- eDirectory 8.8 SP8 Patch 4
- iManager 2.7 SP7 Patch 3
- Java 1.7.0.72

1.2 Fixed Issues

This release includes software fixes in the following components:

1.2.1 Administration Console

The following issues are fixed in the Administration Console:

1.2.1.1 Curly Bracket in URL Leads to Policy Evaluation Failure and User is Logged Out

Issue: If the URL in Administration Console contains an unescaped curly bracket ({}) it leads to a policy evaluation failure and the user is denied access.

Fix: This issue is fixed and now unescaped curly brackets are allowed in authorization policy URLs. [Bug 895264]

1.2.1.2 Error Message Displayed With x509 Authentication is Not Localized

Issue: When the x509 authentication is configured, all error messages are in English and are not localized.

Fix: With this fix, when x509 authentication is configured all the error messages are localized. [Bug 895003]

1.2.1.3 Cross-Site Scripting Vulnerability Issue in JSP Pages

Issue: Multiple cross-site vulnerabilities exist in `debug.jsp` page. The affected URLs are:

- `https://<host>:8443/roma/jsp/debug/debug.jsp?xss=%3Cscript%3Ealert%28%27xss%27%29%3C/script%3E`
- `https://<host>/sslvpn/applet_agent.jsp?lang=%22%3E%3Cscript%3Ealert%28%27xss%27%29%3C/script%3E`

Fix: This issue is resolved by sanitizing `.jsp` pages in the affected URLs. [Bug 911030][CVE-2014-5214]

1.2.1.4 Cross-Site Scripting Issue Injects Script to the Auditing Page

Issue: The Auditing page is vulnerable to cross-site scripting attacks. The affected URL is:

```
https://<host>:8443/roma/system/cntl?handler=dispatcher&command=auditsave&&secureLoggingServersA='){}};alert('xss');function+x(){if('&port=1289
```

Fix: This the issue is resolved by sanitizing the affected URL. [Bug 911027][CVE-2014-5216]

1.2.1.5 JSP Pages Display Sensitive Information to an Authenticated Administrator

Issue: An administrator can view internal credential details by using specific .jsp pages. The affected URLs are:

- https://<host>:8443/roma/jsp/volsc/monitoring/dev_services.jsp
- https://<host>:8443/roma/jsp/debug/debug.jsp

Fix: This issue is resolved by decrypting the credential information in the affected URLs and sensitive information is not displayed to the administrator. [Bug 911029][CVE-2014-5215]

1.2.2 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: Multiple cross-site scripting vulnerabilities exist in the x509err.jsp page of the following URL:

```
https://<host>/nidp/jsp/x509err.jsp?error=%3Cscript%3Ealert%28%27xss%27%29%3C/
script%3E
```

Fix: This issue is resolved by sanitizing the x509err.jsp page in the affected URL. [Bug 911028][CVE-2014-5216]

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

Issue: Cross-site scripting vulnerability affects the WS-Federation authentication process in the following URL:

```
cbcxt=&popupui=&vv=&username=fumail01%40basf.com&mkt=&lc=&wfresh=&wa=wsignin1.0&wt
realm=urn:federation:MicrosoftOnline&wctx=ernw"><script>alert
```

Fix: This issue is resolved by replacing the .jsp file in the affected URL. [Bug 911031]

1.2.2.3 JCC Port 1443 Accepts SSLv3 Requests

Issue: In the Identity Server, the JCC port 1443 is affected by POODLE vulnerability as it accepts SSLv3 requests. (CVE-2014-3566)

Fix: This release fixes the POODLE vulnerability by disabling SSLv3 requests on the JCC port 1443. [Bug 909952]

1.2.3 Access Gateway

The following issue is 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)

Fix: This release fixes the Poodle vulnerability by disabling SSLv3 requests on the JCC port 1443. [Bug 909952]

2 Upgrading to 3.2 SP3 HF1

IMPORTANT: Ensure that you are currently on Access Manager 3.2 SP3 before upgrading to Access Manager 3.2 SP3 HF1.

To upgrade Access Manager Appliance 3.2 SP3 HF1, perform the below steps:Access Manager Appliance

1. Go to NetIQ Downloads Page.
2. Under **Patches**, click **Search Patches**.
3. Specify `AM_32_SP3_HF1.zip` in the search box and download the file.
4. Save the 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 using the `unzip <patch name>.zip` command, where <patch filename> is the name of the patch file, for example, AM_32SP3_HF1.

   For more information about the upgrade process, see Upgrading Access Manager Appliance 3.2 SP2 Using the Patch Process.
6. Run the `sh installPatch.sh` command. This command installs the patch and the bundled binaries.

   To install 3.2 Service Pack 3, see the NetIQ Access Manager Appliance 3.2 SP3 Installation Guide.

   For more information about upgrading Access Manager Appliance 3.2 SP3, see Upgrading Access Manager Appliance.

3 Verifying Version Numbers

It is important to verify the version number of existing Access Manager components before you upgrade or migrate to 3.2 Service Pack 3 HF1. This ensures that you have the correct version of files on your system.

- Section 3.1, “Verifying Version Number Before Upgrading to 3.2 SP3 HF1,” on page 4
- Section 3.2, “Verifying Version Number After Upgrading to 3.2 SP3 HF1,” on page 4

3.1 Verifying Version Number Before Upgrading to 3.2 SP3 HF1

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*
2. Examine the value of the Version field to see if it displays a version that is eligible for upgrading to 3.2 Service Pack 3 HF1. The version field should list 3.2.3-47.

3.2 Verifying Version Number After Upgrading to 3.2 SP3 HF1

1. In the Administration Console, click **Access Manager** > **Auditing** > **Troubleshooting** > **Version**
2. Verify that the **Version** field lists 3.2.3-47 + HF1-66.

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

4.1 Cross-Site Request Forgery Script Allows Password of an Authentication Administrator to be Changed

Issue: An attacker can issue a GET request and change the password of an authentication administrator. `[CVE-2014-5217]`

Workaround: This issue will be fixed in the next release of NetIQ Access Manager. For more information, see TID 7015997

4.2 Cross-Site Scripting Vulnerability Allows Attacks on URLs

Issue: Cross-Site scripting vulnerability affects the following URLs: `[CVE-2014-5216]`

- `https://<host>:8443/nps/servlet/webacc?taskId=dev.Empty&merge=dm.GenericTask&location=/roma/jsp/admin/view/main.jss'%2balert+('xss')%2b'`
- `https://<host>:8443//nps/servlet/webacc?taskId=debug.DumpAll&xss=%3Cimg%20src=%22/404%22%20onerror=%22alert+%28%27xss%27%29%22%3E`

Workaround: This issue will be fixed in the next release of NetIQ Access Manager. For more information, see TID 7015994

4.3 Issue with NTLM Authentication

Issue: Authentication fails when you access a protected resource that uses NTLM authentication. `(Bug 867593)`

Workaround: None

4.4 Issue with the Audit Logging Server

Issue: The Access Gateway health reports the Audit Logging Server service as green with a message indicating it is operational even though the Audit Server is not running. `(Bug 878552)`

Workaround: None

4.5 Upgrading the Primary or Secondary Administration Console to 3.2 SP3 Throws an LDAP Bind Error

Issue: Upgrading the primary/secondary Administration Console throws an `ldap_bind : Can't contact LDAP server` error. `(Bug 887213)`

One of the causes of this issue is because the validity of the eDirectory server certificate has expired.

Workaround: From the eDirectory server terminal execute the following commands:

1. `ndsconfig upgrade` [This creates new certificates for the server]
2. `nldap -u` [This unloads and stops LDAP services]
3. `nldap -l` [This command starts and loads the LDAP services]

   After executing these commands, the upgrade proceeds without issues.

5 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).

6 Legal Notice