TRIDIUM

Niagara AX 3.5 and 3.6 Security Patches

December 18, 2012

UPDATE

Tridium is releasing an update to its August 10 patch for NiagaraAX versions 3.5 and 3.6.

This Security Patch is now available and updates the previous patch. Tridium strongly recommends ALL customers apply the new patch, including those customers who installed the August 10 patch.

Summary

This is a security patch to Niagara AX 3.5 and 3.6 that addresses vulnerabilities associated with the Security Alert released by Tridium on July 13, 2012. Installation instructions for the patch are included at the end of this document. The patch includes changes in certain default settings and user access that may require additional action by users. Tridium strongly recommends reading this document carefully to understand and anticipate these changes before applying the update.

> **Note**
>
> **Regarding Appliances and other 3rd party content:**
>
> **This patch is not available for the Niagara Enterprise Security (access control) products. These products will require separate patches to be available at a later date. Tridium recommends users manually apply the configuration changes listed below when possible.**
>
> **For appliances and custom modules supplied by Tridium partners, please contact the content provider regarding compatibility before applying the security patch.**

Release Notes

Changes to User Permissions:

In general, no functionality is removed by either the version 3.5 or 3.6 security patch. However, certain features may need a higher user permission level than before.

- Only users with "Super User" privileges are allowed to add a new User Service, such as the RSA or LDAP services, to a running station.

- In the New Station Wizard, the default Category Service is configured such that many Niagara objects are placed in an "Admin" category (Category 2). Best practices recommend that permissions to access objects in this category, such as the root station folder, are restricted to users with "Admin" privileges or higher. See the NiagaraAX User Guide section "Permissions Browser" for details on configuring user permissions for categories.
- By default, the ability to add or edit Program Objects is restricted to users with Super User privileges. NonSuper Users can still access the properties and invoke the actions of existing Program Objects.
    - Super User privileges are required to add or edit Robots or Provisioning Robots. Super User privileges are also required by the user account in each subordinate station that a Supervisor uses to make a client connection during provisioning.
    - An advanced use of Export Tags may require copying a Program Object when Joining a JACE to a Supervisor. The user performing the Join must have Super User privileges in order for the Export Tag to function correctly.

Changes to Passwords:

- When a user opens a station in Workbench for the first time, the "Remember these credentials" checkbox in the login (Authentication) dialog is no longer enabled by default.
- The "Require strong passwords" property is now enabled by default on the Niagara User Service. Once logged in, users with Admin privileges can disable the strong password requirement if desired. A strong password has a minimum of 8 characters with at least one numeric or special character and one alphabetic character.
- The New Station Wizard requires a strong password for the Admin user. Blank passwords are no longer allowed.

Changes to File Access:

- Certain files available before applying this patch are no longer accessible as a result of new blacklisting policies. Blacklisted files are not available through remote station access (i.e., network access via Fox or a Web Browser). Only platform users can access blacklisted files.
- Platform users can modify the blacklisting policies. Details on how to edit the host's system.properties file to blacklist files by name or path will be in an upcoming revision of the NiagaraAX Platform Guide. For now, see comments in your local system.properties file.
- Remote station access to config*.bog files is no longer allowed, even for users with Super User privileges or users with admin privileges on the station's File space. Platform users can still access these files through a platform connection.
- The default Authentication Scheme for web access has changed from "Cookie" to "Cookie Digest", as specified in a station's Web Service. As a result, custom login templates may need to be modified to work properly. Although this setting can be changed back to cookie, it is against IT security best practices and is not recommended. However, there may be scenarios when a user needs to set the Authentication Scheme back to Cookie:
    - if the "domain-wide cookies authentication" feature with the regular User Service is used
    - if the LDAP User Service or Active Directory User Service is used

Installation Instructions

Customers with Niagara systems older than 3.5 or with earlier releases of 3.5 or 3.6 should first upgrade to the latest version of the Niagara Framework software. This means for AX 3.5 installations you must be running 3.5.39 or greater. For AX 3.6 installations you must be running 3.6.47 or greater.

For a Niagara Supervisor or Workbench:

1. Download the appropriate zip file for the Niagara AX version to be patched.
   a. For 3.5 download the 3.5 Security Patch.
   b. For 3.6 download the 3.6 Security Patch.
2. Start Workbench and open a platform connection to the local host.
3. Open the Application Director view and stop any running stations.
4. Close all instances of Workbench.
5. Extract the zip file to the "modules" directory of the Niagara AX installation on your PC or laptop. (Ex. C: \Niagara\Niagara-3.6.47\modules).
6. If patching a Niagara Supervisor:
   a. Restart the supervisor station.
   b. Login to the patched supervisor station and review the configuration per the change details listed above.

For an embedded Niagara controller (JACE):

1. Start Workbench on a Niagara instance that has been patched as described above.
2. Open a platform connection to a Niagara Controller to be updated.
3. Open the Software Manager view.
4. Update the out of date modules. The specific modules included in the patch are: backup, baja, bql, control, crypto, fox, net, niagaraDriver, obixDriver, pdf, program, wbutil, web, and workbench.
5. Reboot the Niagara controller.
6. Login to the patched Niagara controller and review the configuration per the change details listed above.

Legal

Information and/or specifications published here are current as of the date of publication of this document. Tridium, Inc. reserves the right to change or modify specifications without prior notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia. Products or features contained herein are covered by one or more U.S. or foreign patents. This document may be copied by parties who are authorized to distribute Tridium products in connection with distribution of those products, subject to the contracts that authorize such distribution. It may not otherwise, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Tridium, Inc. Complete confidentiality, trademark, copyright and patent notifications can be found at: http://www.tridium.com/galleries/SignUp/Confidentiality.pdf

JACE, Niagara Framework, Niagara AX Framework and the Sedona Framework are trademarks of Tridium, Inc.

3951 Westerre Parkway, Suite 350 Richmond, VA 23233
Phone: 804.747.4771 Fax: 804.747.5204