Please Update Your Niagara Software: JNLP/Web Start Vulnerability

Security Bulletin #: SB 2021-Tridium-1

Defect#: PSIRT-668

CVSSv3: 5.6-6.4 (AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N - AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)

Summary

The supported versions of Niagara listed in this technical bulletin have been identified to have a vulnerability related to Java Network Launch Protocol (JNLP), a component used in Java Web Start. As a result, support for Java Web Start and the associated Niagara Applet has been removed with the patched versions listed in this bulletin. These patches also include a new security control which was added to the Web Service to provide additional validation of the HTTP Host Header field.

Tridium first announced that support for Java Web Start was going to be phased out in February 2019 via a Customer Bulletin. At that time, we advised our customers to use other options. Now, due to discovery of the JNLP vulnerability, it is imperative that customers migrate off Java Web Start as soon as possible. Java Web Start support was removed from Niagara 4.9 and Niagara EntSec 4.9, so these newer releases are not impacted by this vulnerability. Niagara 4.10 is not impacted by this vulnerability and already has the patched functionality included in the release.

Regarding the new security control added to the Web Service, Niagara developers have added the ability to validate the 'Host' header for incoming HTTP/S requests to a Niagara station. Disabled by default, Host Header Security Control can be enabled in the Web Service > Host Header Validation Settings. Once enabled, any incoming HTTP/S request will have its 'Host' header validated against the comma-separated list specified in the Host Header Validation Settings > Valid Host Headers. In addition to the items specified in the list, the various local IP addresses corresponding to the station will also be considered valid. Any request that does not pass validation will be rejected with a 400 error.

Please continue to use Niagara Web Launcher for viewing any WbWebProfiles.

Supported Product	Patch Versions
Niagara AX 3.8.504	web-3.8.504.1.jar
Niagara 4.4.94.14	baja-4.4.94.14.6.jar jetty-rt-4.4.94.14.1.jar web-rt-4.4.94.14.4.jar
Niagara 4.8.0110.5	jetty-rt-4.8.0.110.1.jar web-rt-4.8.0.110.5.jar

Niagara 4.9.130.2	jetty-rt-4.9.1.30.1.jar web-rt-4.9.1.30.1.jar
Niagara EntSec 2.3.303	web-3.8.504.1.jar
Niagara EntSec 2.4.44.1	baja-4.4.94.14.6.jar jetty-rt-4.4.94.14.1.jar web-rt-4.4.94.14.4.jar
Niagara EntSec 4.8.0.34	jetty-rt-4.8.0.110.1.jar web-rt-4.8.0.110.5.jar
Niagara EntSec 4.9.0.60	jetty-rt-4.9.0.198.2.jar web-rt-4.4.94.14.4.jar

Recommended Action

Tridium recommends adopting the patches identified above or upgrading to Niagara 4.10 and Niagara Enterprise Security 4.10. In addition to applying the patches, Tridium recommends enabling the new Host Header Security Control (Host Header Validation) in the Web Service.
These updates are available by contacting your sales support channel or the Tridium support team at support@tridium.com.

It is important that all Niagara customers for all supported platforms update their systems with these releases to mitigate risk. If you have any questions, please contact your Tridium account manager or Customer Support at support@tridium.com. Again, all Niagara customers that are not running a supported platform should update their systems to a supported release – preferably Niagara 4.10.

Mitigation

In addition to updating your system, Tridium recommends that customers with affected products take the following steps to protect themselves:

- Review and validate the list of users who are authorized and who can authenticate to Niagara.
- Allow only trained and trusted persons to have physical access to the system, including devices that have connection to the system though the Ethernet port.
- If remote connections to the network are required, consider using a VPN or other means to ensure secure remote connections into the network where the system is located.

Cybersecurity is a priority at Tridium. We are dedicated to continuously improving the security of our products, and we will continue to update you as we release new security features, enhancements, and updates.

Acknowledgement

Tridium would like to acknowledge Ken Pyle and the team at Cybir for reporting this vulnerability to us.

March 2021

niagara marketplace niagara community tridium university

ABOUT US

For almost 20 years, Tridium has led the world in business application frameworks — advancing truly open environments that harness the power of the Internet of Things. Our products allow diverse monitoring, control and automation systems to communicate and collaborate in buildings, data centers, manufacturing systems, smart cities and more. We create smarter, safer and more efficient enterprises and communities — bringing intelligence and connectivity to the network edge and back.

tridium.com