Please Update Your Niagara Software: Hx Profile Vulnerability

Security Bulletin #: SB 2022-Tridium-1

Defect#: NCCB-55568

CVSSv3: 5.5 (Medium | AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L)

Summary

The following patches resolve a security issue affecting users that use any Hx Profile (HTML5 Hx Profile, Default Hx Profile, etc.) to access a Niagara station through the browser. This could allow remote execution of a script in the client's browser. This applies to all supported versions of Niagara (Niagara 4.10 and Niagara 4.11) and may impact unsupported versions as well. Tridium strongly recommends that you apply the most recent patch for your version of Niagara.

Solution

Tridium has developed a fix for the vulnerability which is available as a separate patched web-rt.jar module. The relevant patched web-rt.jar module needs to be added to installations running current supported versions of Niagara releases (Niagara 4.10u1 and Niagara 4.11). Future releases of supported versions will include the fix and not require this patch to be applied separately.

Recommended Action

- Installations of Niagara 4.10u1 and Niagara Enterprise Security 4.10u1 should install the web-rt.jar version 4.10.1.36.1 (or later)
- Installations of Niagara 4.11 and Niagara Enterprise Security 4.11 should install the web-rt.jar version 4.11.0.142.1 (or later)
- Installations of earlier/unsupported Niagara versions should be upgraded to one of the supported versions above and the relevant patch module applied.

These updates are available on the Niagara Central download site, by contacting your sales support channel, or by contacting 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 contact Customer Support via support@tridium.com.

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.
- Consider using a VPN or other means to ensure secure remote connections into the network where the system is located, if remote connections are enabled,
- Sign all modules and program objects provided by third-party teams.
- Review the Niagara Hardening Guide and implement the recommended techniques for securing your installation.

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.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION IN THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- TRIDIUM RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- TRIDIUM PROVIDES THE CVSS SCORES 'AS IS' WITHOUT WARRANTY OF ANY KIND. TRIDIUM DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL TRIDIUM BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT. SPECIAL, OR CONSEQUENTIAL DAMAGES.

February 2022

DISCOVER. CONNECT. ACHIEVE.

niagara marketplace   niagara community   tridium university

ABOUT US

Tridium is a global leader 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

If you no longer wish to receive Tridium marketing communications, click here: Unsubscribe

Privacy Statement

© 2022 Tridium Inc.