Please Update Your Niagara Software: Cross-Site Scripting Vulnerability

Security Bulletin #: SB 2018-Tridium-2
CVSS v3.0 Base Score: 5.7 (AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N)
Defect #: NCCB-36761

Summary

A cross-site scripting vulnerability was discovered in the Niagara web interface which could allow an authenticated user to inject client-side scripts into some web pages that could then be viewed by other users.
No known exploitation of the vulnerability have been identified.
We have made modifications to the application to remove the vulnerability and recommend that users update to the version identified below.

Recommended Action

Tridium has released new patches that mitigate this vulnerability. Tridium strongly recommends that users apply these patches to their corresponding Niagara installations to mitigate this risk.

Product	Consolidated Patch Set Version	Consolidated Patch Set
Enterprise Security 2.3u1	2.3.118.6	https://software.niagara-central.com/ord?portal:/download/6284
Niagara AX 3.8u4	3.8.401.1	https://software.niagara-central.com/ord?portal:/download/6276
Niagara 4.4u2	4.4.93.40.2	https://software.niagara-central.com/ord?portal:/download/6268
Niagara 4.6	4.6.96.28.4	https://software.niagara-central.com/ord?portal:/download/6281

These patches are available 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 should 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.

Acknowledgement

Tridium would like to acknowledge Daniel Santos and Elisa Costante of SecurityMatters for reporting this vulnerability to us.

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS, but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 -8.9
Critical	9.0 - 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

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.

DISCOVER. CONNECT. ACHIEVE.

niagara marketplace niagara community tridium university

ABOUT US

For more than 15 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