Please Update Your Niagara Software: Chromium Vulnerability

Security Bulletin# SB 2019-Tridium-1
CVSS v3.0 Base Score: 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/i:H/A:H)
Defect# NCCB-39792

Summary
A vulnerability was discovered in Chromium (CVE-2019-5786) that allows for code execution while rendering using the FileReader API. Chromium is a core component used for rendering HTML pages in Workbench using jxBrowser. Niagara-supported releases that are impacted by this vulnerability are Niagara 4.4u2, Niagara 4.6, and Niagara 4.7.

Reports of exploits of Chromium have been reported as targeting Windows 7, 32-bit platforms; however, exploits on other platforms may also occur.

We have updated Chromium (via an update to jxBrowser) to remove the vulnerability and recommend that users update to the versions identified below.

Recommended Action
Tridium has released new updates that mitigate this vulnerability.

Product	Update Version	
Niagara 4.4U3	4.4.94.14	Release Notes
Niagara 4.7u1	4.7.110.32	Release Notes

Current users of Niagara 4.6 are encouraged to update to Niagara 4.7u1.

NOTE: 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 take the following protective steps:

- 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.

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 AND USERS 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