Update Your Niagara Software to Address libwebp Vulnerability

Security Bulletin #: SB 2024-Tridium-1
Defect#: PSIRT-942 (CVE-2023-4863)
CVSSv3: 6.8 (Medium | AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H)

Summary

The following releases of Niagara Framework® have been updated to address a vulnerability in the libwebp component utilized by jxBrowser. The CVE reported is CVE-2023-4863 and has been rescored as 6.8, based on the libwebp component's usage in Niagara.

Solution

Tridium has updated the version of jxBrowser shipped with Niagara to address the identified vulnerability.

Recommended Action

Please update any installations of Niagara to one of the following versions.

- Niagara Framework 4.10u7
- Niagara Enterprise Security 4.10u7
- Niagara Framework 4.13u2
- Niagara Enterprise Security 4.13u2

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.

January 2024

DISCOVER. CONNECT. ACHIEVE.

niagara marketplace niagara community tridium university

ABOUT US

Tridium is a world 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

© 2024 Tridium Inc.