Niagara Software: QNX BadAlloc Vulnerability - New Items

Attention All Lynxspring Technology and Business Partners:

Please be advised that the following two items have been added to this Advisory that was previously sent on August 31, 2021.

- A medium-level Privilege Escalation vulnerability has been identified in QNX code used in Niagara platforms prior to Niagara 4.10u1. Exploitation of this vulnerability does not expose any additional functionality or data. An update has been made to Niagara platforms to mitigate this vulnerability.
- In addition, a handful of vulnerabilities were identified in the Chromium version embedded in jxBrowser. All Niagara-based platforms prior to Niagara 4.10u1 are impacted.

August 31, 2021

Attention All Lynxspring Technology and Business Partners:

We have been advised by Tridium that Blackberry QNX has revealed an integer overflow that impacts QNX OS version 6.50 SP1 and earlier (CVE-2021-22156). **See the CISA Alert**.

All QNX-based Niagara Framework® platforms **prior to Niagara 4.8 are impacted, except for Lynxspring's JENEsys® Edge™ series controllers**.

Due to compensating controls in Niagara, the CVSS score for this vulnerability has been recalculated to be 3.9 and is classified as a low risk.

Recommended Action

Tridium recommends upgrading to Niagara 4.10u1. These updates are available by contacting our orders team at **https://orders@lynxspring.com**. For additional questions, contact our support team at**https://support@lynxspring.com**. If a current SMA is in place, then there is no cost for the upgrade.

It is important that all Niagara customers for all supported platforms update their systems with these releases to mitigate risk. As always, we highly recommend that customers running on an unsupported platform (such as Niagara AX) take action to update their systems to a supported version.

Mitigation

In addition to updating your system, Lynxspring 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** which is available on our Resources site at:**https://resources.lynxspring.com/cyber-security/798-niagara-4-hardening-guide/viewdocument/798** for techniques on securing your installation.

Cyber security is a priority at Lynxspring. We are committed to taking a strong leadership role in helping our partners maintain a strong posture and helping them ensure the cyber protection of their building automation systems, equipment, and devices.

Sincerely,

Marc Petock
Chief Marketing & Communications Officer
Lynxspring, Inc.
Phone: 877-649-5969
marc.petock@lynxspring.com
www.lynxspring.com