Security Bulletin

SecB0002: Niagara JACE, Edge 10 QNX Vulnerabilities

Summary

First published: September 10, 2019

Description	Two vulnerabilities have been discovered in the QNX operating system images distributed by Tridium.
Affected Products	Niagara AX 3.8u4 (JACE 3e, JACE 6e, JACE 7, JACE-8000) Niagara 4.4u3 (JACE 3e, JACE 6e, JACE 7, JACE-8000) Niagara 4.7u1 (JACE-8000, Edge 10)
Recommended Action	Update your Niagara Software
CVSS v3.0 Base Score	4.4 / 8.0

Description

Two vulnerabilities have been discovered in the QNX operating system images distributed by Tridium.

The first vulnerability is related to a vulnerability that could allow a less privileged process to gain read access to privileged files.

The second is related to a vulnerability in the QNX procfs service that could allow a less privileged process to gain access to a chosen process's address space.

For further details refer to technical bulletin SB 2019-Tridium-3 on the Tridium website.

Security Bulletin

Recommended Action

1. Update your Delta Niagara Supervisor Software to at least version 4.7.110.32.
2. Install the Qnx Security Patches for HAREMB-1220 and 1221.

   Note: Delta Niagara Supervisor version 4.8.0.110.5 already includes these patches.
3. Upgrade/recommission affected JACE/Edge 10 controllers.

Mitigation

In addition to upgrading your Delta Niagara 4 software, Delta Controls recommends the following actions to secure your building sites:

- Do not leave building controllers exposed to the Internet.
  - If remote connections to the network are required, use a Virtual Private Network (VPN).
  - Secure your network using Tempered Networks products (available through Delta Controls).
- Regularly review and validate the list of users who are authorized to access sites and controllers.
- Ensure personnel with access to the system are knowledgeable about and are trained to use Niagara products and networks.
- Follow the security industries recommended practices for securing your sites. https://ics-cert.us-cert.gov/Recommended-Practices

Download

Niagara Supervisor Software and Qnx Security Patches for HAREMB-1220 and 1221 can be downloaded from the Software Downloads page on the Delta Support website.

Detailed instructions can be found in the patch zip files.

Appendix: About CVSS

All CVSS scores can be mapped to the qualitative ratings defined by the Qualitative Severity Rating Scale table (see below):

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

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments. The Base group is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.

- The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. On the other hand, the Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.
- The CVSS v3.0 vector string is a text representation of a set of CVSS metrics. It is commonly used to record or transfer CVSS metric information in a concise form.

For more information, visit the CVSS website at: http://www.first.org/cvss/.