August 27, 2019

Please Update Your Niagara Software: QNX Vulnerabilities

Security Bulletin# SB 2019-Tridium-3
CVSS v3.0 Base Score: 4.4 (AV:L/AC:L/PR:H/UI:N/S:U/C:H/i:N/A:N)
Defect# HAREMB-1220
CVSS v3.0 Base Score: 8.0 (AV:L/AC:H/PR:H/UI:N/S:C/C:H/i:H/A:H)
Defect# HAREMB-1221

Summary
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.

The following supported platforms are impacted:

- 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)

NOTE: Niagara Windows and Linux Supervisor installations are not impacted.

We have updated the QNX OS images to remove the vulnerability and recommend that users update to the versions identified below:

Recommended Action
Tridium has released new updates that mitigate these vulnerabilities.

Product	QNX Patches
Niagara AX 3.8u4	OS Dist: 2.7.402.2 NRE Config Dist: 3.8.401.1
Niagara 4.4u3	OS Dist: 4.4.73.38.1 NRE Config Dist: 4.4.94.14.1
Niagara 4.7u1	OS Dist: (JACE 8000) 4.7.109.16.1 OS Dist (Edge 10): 4.7.109.18.1 NRE Config Dist: 4.7.110.32.1

These updates 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.

August 27, 2019

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.