US Coast Guard Cyber Command
Maritime Cyber Alert 02-21

August 17, 2021

Information Sharing Protocol: TLP-White (https://www.us-cert.gov/tlp)

"BADALLOC" CRITICAL VULNERABILITY: BLACKBERRY QNX & MORE

Summary: The recent public disclosure from BlackBerry regarding the "BadAlloc" vulnerability in their QNX OS versions 6.5 and earlier, should put all organizations on continued alert for threats and vulnerabilities to the cyber landscape. "BadAlloc" is the name assigned to the family of vulnerabilities discovered in embedded Internet of Things (IoT) and Operational Technology (OT) operating systems and software to describe a class of memory overflow vulnerabilities.

An embedded system is a computer implemented as part of a larger system. It is typically designed around a limited set of specific functions in relation to the larger system and it may consist of the same components of a typical computer, or be just a microcontroller.

A device with these exploitable vulnerabilities may enable malicious actors to deny system availability, ex-filtrate data, and move laterally within the systems in which they are installed. These malicious actions can lead to consequences for systems and their users, ranging from loss of data and trust, to physical harm and loss of life.

BlackBerry QNX is the most recent organization to disclose this vulnerability, however there are several other products that have the same "BadAlloc" vulnerability. The Maritime community should be examining their systems to determine if they contain BlackBerry QNX versions 6.5 or below, or **any of the other products identified by CISA listed in ICSA-21-119-04: Multiple RTOS (Update B).**

Mitigations:

There are two significant challenges with mitigating this vulnerability. The first is identifying the systems and products that have vulnerable software. Because this vulnerability is most prevalent in embedded systems, it may not be readily apparent that your organization has this vulnerability.

Each organization is strongly encouraged to extensively review their systems and to identify any that contain vulnerable software/operating systems.

The second challenge relates to applying updates. The best solution for mitigating this vulnerability is upgrading to a new, non-vulnerable version. For example, upgrading QNX to version 6.6 or higher mitigates the vulnerability. However, many of the systems running QNX and these other real-time operating systems (RTOS) vulnerable software may be difficult to upgrade due to required downtime.

If you are able, the best mitigation is to upgrade to a secure version of the vendor's software, but before doing so, first compute the hash values of the upgraded software and verify that they match the values published by the vendors. Additionally, thoroughly test the upgraded software in a sandboxed environment on isolated devices to ensure that the new software does not negatively affect or render inoperable any devices that it will be loaded on and interact.

If operations do not permit the downtime required to apply the needed upgrade, or an upgrade is not available, it is recommended that appropriate controls are identified and implemented to mitigate the risks. Potential controls may include:

- Limiting remote access to the vulnerable devices, and understanding even "secure" methods such as Virtual Private Networks may have other vulnerabilities.
- Ensuring vulnerable devices are not accessible from the internet.
- Placing vulnerable control system networks and remote devices behind firewalls and isolating them from business networks.

Additionally, it is recommended to not only implement controls to protect from exploitation, but ensure that software and hardware inventory policies are current and adequate. Quick identification of vulnerable systems is critical to prevent threat actors from damaging critical systems. Many applications and devices may run on QNX, but require research to confirm if this vulnerability is present. A complete understanding of components that make up your critical systems, and a comprehensive inventory will assist in quickly identifying risks to your organization.

Resources:

If your organization identifies a vulnerability or has any questions related to this alert, such as technical assistance with the mitigation actions, please contact U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at 202-372-2904.