**August 17, 2021**

# Joint WaterISAC – U.S. Environmental Protection Agency Advisory

## BadAlloc Vulnerability Impacting BlackBerry QNX RTOS

On Tuesday, August 17, 2021 the Cybersecurity and Infrastructure Security Agency (CISA) published an alert highlighting a vulnerability named "BadAlloc" (CVE-2021-22156) that has been identified in the BlackBerry (BB) QNX Real Time Operating System (RTOS) that is used in a wide range of Industrial Control Systems (ICS). Additionally, several other manufacturers have developed their own proprietary versions of this RTOS using similar technology to the BB QNX, which leaves their products vulnerable to the BadAlloc flaw as well.

**Attention:** *Every water and wastewater utility should determine the presence of impacted RTOS devices within their environments. Asset owners are encouraged to check this original CISA ICS Advisory (ICSA-21-119-04) Multiple RTOS (Update B) for a partial list of impacted products. In addition, asset owners should work with IT and OT support staff, system integrators, and ICS and IoT manufacturers to determine if any process control systems are vulnerable to this flaw and consider patching or applying appropriate compensating controls/workarounds immediately until a patch can be applied.*

**What you need to know.**

- A high-risk vulnerability impacting real-time operating systems (RTOS's) known as BadAlloc has been identified in BlackBerry QNX RTOS Versions 6.5 SP1 and earlier.
- BadAlloc was originally disclosed by Microsoft in April 2021 as a type of remote code execution vulnerability affecting Internet of Things (IoT) devices and industrial equipment that is specifically used in industrial/OT, medical, and corporate networks.
- In May 2021, CISA issued a public disclosure regarding BadAlloc and its impact to RTOS's in other manufacturer's products.
- BlackBerry states that QNX RTOS is used in more than 500 million endpoint products, including more than 300 million embedded systems around the world across a range of industries such as aerospace, defense, automotive, commercial vehicles, heavy machinery, industrial controls, medical, rail, and robotics. Visit BlackBerry for a list of affected products.
- Given widespread usage among industrial control systems, it is important for water and wastewater sector entities to assess their environments for deployment of vulnerable components.

**Why is this a concern?**

- If exploited, semi-skilled cyber threat actors can potentially leverage this vulnerability to deny system availability, exfiltrate data, seize control of ICS components, and move laterally within the system(s) and network(s) connected to the vulnerable components.
- While critical infrastructure sectors believed to be most impacted include automotive, transportation, healthcare, energy, and defense, the full extent of the exposure is difficult

to ascertain due to widespread installation of RTOSs across multiple vendors and products, including those that may use proprietary versions.
- Impacted device(s) may need to be taken offline/out-of-service to patch; therefore, patches for this vulnerability may not be applied quickly, leaving organizations exposed.

**Is the disclosed vulnerability patched?**

- BlackBerry has developed software updates to address the BadAlloc vulnerability.
- For a list of known affected products and their patch availability/mitigation actions, visit https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04.
- For patch availability for other RTOS products running in your environment, reach out to system integrators, and ICS and IoT manufacturers.

**Is this vulnerability being actively exploited?**
No active exploitation is known at this time. However, once vulnerability disclosures are made public, the risk of exploitation increases until patches are applied across vulnerable systems.

**Recommended Actions**
Patching is the most effective way to reduce or eliminate the risk from this vulnerability. However, as utilities assess systems for impact and work to install available patches, the following basic cybersecurity hygiene practices may mitigate and detect exploitation:
- Limit or block access to the RTOS at the device or network level.
- Ensure that only ports and protocols used by the application with the RTOS are accessible, blocking all others.
- Implement network segmentation best practices and ensure devices are not accessible from the Internet.
- Conduct frequent vulnerability scanning and intrusion detection monitoring.

**Additional Information**
CISA is available to provide cybersecurity advice and support to entities working to obtain a patch. To request support from CISA, please contact CISAservicedesk@cisa.dhs.gov. For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics or incident reporting: https://uscert.cisa.gov/report.

WaterISAC and EPA will continue to share information with members and partners as more is learned about this vulnerability. Likewise, all water and wastewater utilities are encouraged to share information with WaterISAC by emailing analyst@waterisac.org, calling 866-H20-ISAC, or using the online incident reporting form.

**References**


- https://support.blackberry.com/kb/articleDetail?articleNumber=000082334
- https://us-cert.cisa.gov/ncas/alerts/aa21-229a
- https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04
- https://msrc-blog.microsoft.com/2021/04/29/badalloc-memory-allocation-vulnerabilities-could-affect-wide-range-of-iot-and-ot-devices-in-industrial-medical-and-enterprise-networks/