BlackBerry QNX Software Development Platform (SDP) 6.5.0SP1 Vulnerability|CVE-2021-22156

Publication Date: 08-25-2021
Last Update: 08-25-2021
Current Version: V1.0

Summary

Based on what has been publicly released to this point, and the information from the GE Gas Power Intel team, the vulnerability does not target any GE products specifically. GE currently evaluates this as a lower overall risk to GE Gas Power customers.

BlackBerry recently published vulnerabilities collectively known as “BadAlloc” that details vulnerabilities found in multiple Real-Time Operating Systems (RTOS) and supporting libraries. In order to exploit this vulnerability, an attacker must have control over the parameters to a *calloc()* function call and the ability to control what memory is accessed after the allocation. To remotely exploit this vulnerability, an attacker would require local network access and the devices would need to have a vulnerable service running and exposed.

Impact

The successful exploitation of these vulnerabilities may enable actors to deny system availability or carry out arbitrary code execution.

Vulnerable

From the BlackBerry Security Advisory of August 17, 2021, the affected QNX products and versions include

- QNX SDP 6.5.0SP1
- QNX SDP 6.5.0
- QNX SDP 6.4.1
- QNX SDP 6.4.0
- QNX Momentics Development Suite 6.3.2
- QNX Momentics 6.3.0SP3
- QNX Momentics 6.3.0SP2
- QNX Momentics 6.3.0SP1
- QNX Momentics 6.3.0
- QNX Momentics 6.2.1b
- QNX Momentics 6.2.1
- QNX Momentics 6.2.1A
- QNX Momentics 6.2.0
- QNX Realtime Platform 6.1.0a
- QNX Realtime Platform 6.1.0
- QNX Realtime Platform 6.0.0a
- QNX Realtime Platform 6.0.0

- QNX Cross Development Kit 6.0.0
- QNX Development Kit (Self-hosted) 6.0.0
- QNX Cross Development Kit 6.1.0
- QNX Development Kit (Self-hosted) 6.1.0
- QNX Neutrino RTOS Safe Kernel 1.0
- QNX Neutrino RTOS Certified Plus 1.0
- QNX Neutrino RTOS for Medical Devices 1.0
- QNX Neutrino RTOS for Medical Devices 1.1
- QNX OS for Automotive Safety 1.0
- QNX OS for Safety 1.0
- QNX OS for Safety 1.0.1
- QNX Neutrino Secure Kernel 6.4.0
- QNX Neutrino Secure Kernel 6.5.0
- QNX CAR Development Platform 2.0RR

Recommendation

To minimize the risk that vulnerabilities like BadAlloc represent to the controls network, we recommend the implementation of a good defense-in-depth strategy as detailed in our GEH 6839 Secure Deployment Guide. Some of our recommended controls include:

- Minimize network exposure for all Controllers with the use of network segmentation, placement of controllers behind controls network firewalls and ensure that they are not accessible from the Internet.
- Running the Mark VIe controller(s) in Secure Mode
- Block suspicious external IP addresses at the controls network firewalls. Monitor traffic internally for unusual behavior.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.
- Implement defense-in-depth within the controls network environment consisting of tools such as Intrusion Detection/Prevention Systems (IDS/IPS), firewalls, and network access control (NAC).
- Implement and maintain an anti-malware solution and an endpoint detection and response (EDR) solution.
- Disable remote access services and protocols such as Remote Desktop Protocol (RDP) unless needed. Monitor and restrict remote access usage on a least-privilege basis.
- Have backup and restore processes and procedures in place for disaster recovery and incident response.
- Monitor and maintain account provisioning and access control based on the principle of least privilege

GE Power Product Security Incident Response Team (PSIRT)

Providing secure and reliable products and solutions is vital to the operations of GE Gas Power. Our products are designed with security as a key principle. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect our products and customers. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.

Additional Resources

- CISA ICS Advisory: ICSA-21-119-04: Multiple RTOS
- BlackBerry: QNX-2021-001 Vulnerability in the C Runtime Library Impacts BlackBerry QNX Software Development Platform (SDP), QNX OS for Medical, and QNX OS for Safety

Document History

Version	Release Date	Purpose
1.0	August 25th, 2021	BadAlloc Vulnerability Assessment and Potential Product Impact Statement