BadAlloc Vulnerability Affecting BlackBerry QNX RTOS

SUMMARY

On August 17, 2021, BlackBerry publicly disclosed that its QNX Real Time Operating System (RTOS) is affected by a BadAlloc vulnerability—CVE-2021-22156. BadAlloc is a collection of vulnerabilities affecting multiple RTOSs and supporting libraries.[1] A remote attacker could exploit CVE-2021-22156 to cause a denial-of-service condition or execute arbitrary code on affected devices.[2] BlackBerry QNX RTOS is used in a wide range of products whose compromise could result in a malicious actor gaining control of highly sensitive systems, increasing risk to the Nation's critical functions. **Note**: at this time, CISA is not aware of active exploitation of this vulnerability.

CISA strongly encourages critical infrastructure organizations and other organizations developing, maintaining, supporting, or using affected QNX-based systems to patch affected products as quickly as possible. Refer to the Mitigations section for more information about patching.

TECHNICAL DETAILS

CVE-2021-22156 is an integer overflow vulnerability affecting the `calloc()` function in the C runtime library of multiple BlackBerry QNX products. Exploitation of this vulnerability could lead to a denial-of-service condition or arbitrary code execution in affected devices. 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. An attacker with network access could remotely exploit this vulnerability if the vulnerable product is running and the affected device is exposed to the internet.[3]

CVE-2021-22156 is part of a collection of integer overflow vulnerabilities, known as BadAlloc, which affect a wide range of industries using Internet of Things (IoT) and operational technology (OT)/industrial control systems (ICS) devices. See CISA ICS Advisory ICSA-21-119-04 and Microsoft's BadAlloc blog post for more information.

All BlackBerry programs with dependency on the C runtime library are affected by this vulnerability (see table 1 for a list of affected BlackBerry QNX products). Because many affected devices include safety-critical devices, exploitation of this vulnerability could result in a malicious actor gaining control of sensitive systems, possibly leading to increased risk of damage to infrastructure or critical functions.

Table 1: Affected BlackBerry QNX Products [4]

Product	Affected Version
QNX SDP	6.5.0SP1, 6.5.0, 6.4.1, 6.4.0
QNX Momentics Development Suite	6.3.2
QNX Momentics	6.3.0SP3, 6.3.0SP2, 6.3.0SP1, 6.3.0, 6.2.1b, 6.2.1, 6.2.1A, 6.2.0
QNX Realtime Platform	6.1.0a, 6.1.0, 6.0.0a, 6.0.0
QNX Cross Development Kit	6.0.0, 6.1.0
QNX Development Kit (Self-hosted)	6.0.0, 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, 1.1
QNX OS for Automotive Safety	1.0
QNX OS for Safety	1.0, 1.0.1
QNX Neutrino Secure Kernel	6.4.0, 6.5.0
QNX CAR Development Platform	2.0RR

MITIGATIONS

CISA strongly encourages critical infrastructure organizations and other organizations developing, maintaining, supporting, or using affected QNX-based systems to patch affected products as quickly as possible.

- **Manufacturers** of products that incorporate vulnerable versions should contact BlackBerry to obtain the patch.

- **Manufacturers of products who develop unique versions of RTOS software** should contact BlackBerry to obtain the patch code. **Note**: in some cases, manufacturers may need to develop and test their own software patches.
- **End users** of safety-critical systems should contact the manufacturer of their product to obtain a patch. If a patch is available, users should apply the patch as soon as possible. If a patch is not available, users should apply the manufacturer's recommended mitigation measures until the patch becomes available.
    - **Note**: installation of software updates for RTOS frequently may require taking the device out of service or to an off-site location for physical replacement of integrated memory.

Critical infrastructure organizations are encouraged to review the following guidance for additional information:

- U.S. Coast Guard Maritime Security Advisory: Maritime Cyber Alert 02-21
- U.S. Nuclear Regulatory Commission Security Advisory: Blackberry QNX Vulnerability

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]

CONTACT INFORMATION

For any questions related to this report, please contact CISA at:

- Central@cisa.gov, or
- 1-888-282-0870.

For industrial control systems cybersecurity information, refer to us-cert.cisa.gov/ics.

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams.

REFERENCES

[1] [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]

[2] Ibid.

[3] Ibid.

[4] BlackBerry: QNX. Affected Product List