- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › ICS/OT

BadAlloc Flaw Impacts Many Systems Running BlackBerry's QNX Embedded OS

By Ionut Arghire on August 18, 2021

BlackBerry this week informed customers that the QNX embedded operating system is affected by a BadAlloc vulnerability leading to arbitrary code execution or denial of service.

Publicly disclosed in April, BadAlloc is a collection of 25 vulnerabilities impacting many Internet of Things (IoT) and operational technology (OT) devices. The flaws can allow malicious attackers to gain control of highly sensitive systems.

The issue affects C standard library (libc) implementations, real-time operating systems (RTOS), and embedded software development kits (SDKs), and could be exploited to execute arbitrary code or cause systems to crash.

On Tuesday, BlackBerry revealed that the QNX RTOS is affected by a BadAlloc vulnerability tracked as CVE-2021-22156 (CVSS score of 9.0). The flaw, an integer overflow bug, impacts the C runtime library present in various BlackBerry QNX products.

“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 network access and the devices would need to have a vulnerable service running and exposed,” BlackBerry explains.

QNX, the company says, is used in more than 195 million vehicles, as well as in embedded systems in industries such as aerospace, automotive, defense, industrial controls, and medical, among others.

According to BlackBerry, the issue affects QNX Software Development Platform (SDP) 6.5.0SP1 and earlier versions, QNX for Safety versions 1.0.1 and earlier safety products compliant with IEC 61508 and/or ISO 26262, and QNX for Medical versions 1.1 and earlier safety products compliant with IEC 62304. The company has published a list of affected products.

BlackBerry has released software updates to patch the vulnerabilities, urging all QNX SDP, QNX OS for Safety, and QNX OS for Medical customers to update their products immediately.

Available mitigations include ensuring that all unused ports are blocked, that network segmentation is implemented, and that best practices for vulnerability scanning and intrusion detection are followed. However, no workarounds exist for the vulnerability.

The Cybersecurity and Infrastructure Security Agency (CISA), which notes that the impact of the BadAlloc vulnerability should not be underestimated, encourages organizations using affected QNX-based systems, including critical infrastructure entities, to apply the available patches as soon as possible.

“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,” CISA says.

Related: **Millions of IoT Devices Exposed to Attacks Due to Cloud Platform Vulnerability**

Related: **Devices From Many Vendors Can Be Hacked Remotely Due to Flaws in Realtek SDK**

Related: **August 2021 ICS Patch Tuesday: Siemens, Schneider Address Over 50 Flaws**

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Report: Iranian APT Hexane Targets Israeli Companies
Blockchain Security Company CertiK Raises $24 Million
BadAlloc Flaw Impacts Many Systems Running BlackBerry's QNX Embedded OS
FBI Reportedly Exposed Secret Terrorist Watchlist
Google Awards $42,000 for Two Serious Chrome Vulnerabilities

Tags:

ICS/OT NEWS & INDUSTRY Vulnerabilities IoT Security

Search

Get the Daily Briefing