事　務　連　絡
令和３年８月23日

各都道府県衛生主管部（局）薬務主管課　御中

厚生労働省医薬・生活衛生局医療機器審査管理課

厚生労働省医薬・生活衛生局医薬安全対策課

医療機器のオペレーティングシステムに係る脆弱性への対応について(注意喚起)

今般、厚生労働省大臣官房参事官（サイバーセキュリティ・情報システム管理担当）より、別添のとおり、ブラックベリーQNX リアルタイムオペレーティングシステム(RTOS)バージョン 6.5 SP1 以前において、システムの可用性の支障等に係る脆弱性に関する情報が公表され、医療機器の製造販売業者において、当該脆弱性を標的とした攻撃のリスクについて必要な対応をとるよう、注意喚起されました。

医療機器のサイバーセキュリティ対応については、製造販売業者の責任の下で、設計開発の段階から脆弱性への対応を実施し、かつ、医療機関と連携し、適切な対応を実施する必要があります。ついては、「医療機器のサイバーセキュリティの確保に関するガイダンスについて」（平成 30 年７月 24 日付け薬生機審発 0724 第１号、薬生安発 0724 第１号厚生労働省医薬・生活衛生局医療機器審査管理課長、医薬安全対策課長連名通知)、「国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼)」（令和２年５月 13 日付け薬生機審発 0513 第１号・薬生安発 0513 第１号厚生労働省医薬・生活衛生局医療機器審査管理課長、医薬安全対策課長連名通知）等の関連通知及びガイダンスを参考としつつ、別添に基づき適切な対応を行うよう、貴管下関係事業者に対して周知方御配慮願います。

別添

事　務　連　絡
令和３年８月19日

医薬・生活衛生局医療機器審査管理課長 殿
医薬・生活衛生局医薬安全対策課長 殿
医政局研究開発振興課医療情報技術推進室長 殿

大臣官房参事官
(ｻｲﾊﾞｰｾｷｭﾘﾃｨ・情報ｼｽﾃﾑ管理担当)

ブラックベリーQNX リアルタイムオペレーティングシステム(RTOS)
バージョン 6.5 SP1 以前の脆弱性に対する対応について(注意喚起)

米国国土安全保障省サイバーセキュリティ・インフラストラクチャーセキュリティ庁(CISA)から、2021 年８月 18 日(水)未明(米国時間では８月 17 日(火))にブラックベリーQNX リアルタイムオペレーティングシステム(以下「BBQNXRTOS」という。)のバージョン 6.5 SP1 以前の脆弱性に関する情報が公表されました。

当該 OS の使用範囲には、医療分野も含まれており、この脆弱性が悪用されると、システムの可用性の支障、データ窃取、データ流出、機器の制御の乗っ取り等の被害が発生するおそれがあります。これらを踏まえ、内閣官房内閣サイバーセキュリティセンター(以下「NISC」という。)より、別添のとおり注意喚起が発出されました。

つきましては、NISC からの注意喚起文書(別添)に基づき、より具体的な対策として、下記の対策を実施いただくよう、医療機器の製造販売業者及び医療機関に必要な注意喚起をお願いします。

記

１．医療機器の製造販売業者における対応

（１）パッチ等の入手

自社が製造販売する医療機器において当該脆弱性を悪用されないように、次のとおり対応すること。

ア　脆弱性のあるバージョンを組み込んだ医療機器の製造販売業者は、速やかにブラックベリー社に連絡してパッチを入手すること。

イ　BBQNXRTOS ソフトウェアの独自バージョンを組み込んだ医療機器の製造販売業者は、ブラックベリー社のパッチをベースとした独自のパッチの開発が必要となる場合があるため、その場合は速やかにブラックベリー社に連絡してパッチのソースコードを入手し、独自のパッチの開発等適切に対応すること。

なお、独自のパッチは、適用に先立ちテストする必要があることに留意すること。

（２）利用者への連絡及びパッチの適用

医療機器の製造販売業者は、販売業者と連携の上、利用者に速やかに次のアの事項を連絡し、注意喚起するとともに、イのとおりパッチの適用等必要な措置を講ずること。また､パッチを適用する際には一時的に当該医療機器を利用できなくなることなどを説明すること。

ア　連絡事項

医療機器に組み込まれた BBQNXRTOS には脆弱性があり、当該脆弱性が悪用されると、システムの可用性に支障が生じ、データの窃取、流出、制御の乗っ取り等の被害が発生するおそれがあること。

イ　講ずべき措置

当該医療機器に対して速やかにパッチを適用すること。

また、パッチをすぐに入手できない場合は、パッチを入手するまでの間、製造販売業者が推奨する緩和策を適用すること。

なお、一般的に BBQNXRTOS のアップデートを行うには、当該医療機器の使用を停止する、又は記憶装置を物理的に交換するため、記憶装置を一時取り外すことが必要になる場合がある。

２．医療機関における対応

利用している医療機器において、BBQNXRTOS が利用されていないか、製造販売業者又は販売業者に問い合わせ、利用していた場合は、上記 1.（２）の対応を依頼し、速やかに対策を講じること。対策が完了するまでの間は、当該脆弱性を悪用した攻撃のリスクがあるため、製造販売業者が推奨する対応手順に従って対応すること。本対応には、BBQNXRTOS を使用するアプリケーションが使用するポート及びプロトコルのみにアクセスするようにして、それ以外はブロックするとともに、監視を強化する等により、リスクを低減させることが含まれるものであること。

なお、医療機器に限らず BBQNXRTOS を使用していると思われるものがある場合は、幅広に確認し、対応すること。

３．参考

BlackBerry 社の公式サイト

ア　当該脆弱性に関する情報サイト

https://support.blackberry.com/kb/articleDetail?articleNumber=000082334

イ　当該脆弱性に影響する製品一覧ページ

https://www.qnx.com/support/knowledgebase.html?id=5015Y000001SX2z

ウ　当該脆弱性に対応済みアップデートパッチのダウンロードサイト

https://www.qnx.com/download/

以上

別添

2021 年 8 月 18 日

ブラックベリーQNX リアルタイムオペレーティングシステム(RTOS) バージョン 6.5 SP1 以前の脆弱性の公表について

（内閣官房内閣サイバーセキュリティセンターからの注意喚起抜粋）

1. 概要

本日(8/18(水))未明に米国 CISA 及びベンダーである加国 BlackBerry から以下のとおり、それぞれから公表されましたのでお知らせします。

〇CISA

BadAlloc Vulnerability Affecting BlackBerry QNX RTOS

https://us-cert.cisa.gov/ncas/alerts/aa21-229a

〇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

https://support.blackberry.com/kb/articleDetail?articleNumber=000082334

2. 説明

本脆弱性「BadAlloc」については、米国 CISA が 2021 年 4 月に公開し、JVN で以下のとおり国内で展開されています。

〇JVN

複数の RTOS やライブラリなどにメモリ割り当て処理における脆弱性（"BadAlloc"）

https://jvn.jp/vu/JVNVU90467655/

本日の米国 CISA 等の脆弱性の公表については、これまで幅広い用途に使われている BlackBerry QNX が含まれていませんでしたが、今次、本 RTOS も脆弱性の対象であることを示すものとなります。

このため、事業者等における本脆弱性対応については、今後展開される JVN に従って対応することが求められます。