サイバーセキュリティ通信 Vol.2

令和４年５月

サイバァちゃん

QNAP社製NASを狙ったランサムウェアについて

台湾の電機メーカーである、QNAP社が提供するNAS（ネットワークに接続された記憶装置）に対して、保存されているデータやシステム情報を暗号化し、使用不能にするランサムウェアDEADBOLTによる攻撃が確認されています。

国内においても中小企業を中心に被害が確認されており、業務上必要なデータが使用不能になる等、事業に大きな打撃を与える被害が発生しています。

QNAP社が提供するNASを使用していませんか？

【使用している場合】

QNAP社が提供しているアップデートを適用しているか確認し、まだの場合はアップデートを適用してください。

TS-x51シリーズとTS-x53シリーズの特定の機能（QTS4.3.6とQTS4.4.1）を使用しているNASへの攻撃が発生しており、当該機能に係るアップデートが必要です。

QNAP社の説明

https://www.qnap.com/en-us/security-news/2022/take-immediate-actions-to-secure-qnap-nas-and-update-qts-to-the-latest-available-version

更新方法

https://qnas.znw.co.jp/tutorial/firmware-update/

上記アップデートを適用することがどうしても難しい場合は、NASをインターネットから直接アクセスできないようにしてください。

ランサムウェアの被害を受けた場合、情報が暗号化され身代金を要求されるとともに、その情報が流出するおそれがあります。被害発生時は警察に相談してください。

また、これ以外にもアップデートを行っていない機器がないか確認し、機器の脆弱性等を狙われることがないよう、更新を行いましょう。

長崎県警察本部サイバー犯罪対策課
095-820-0110（3451・3452）
ﾒｰﾙｱﾄﾞﾚｽ e103107@police.pref.nagasaki.jp

サイバー犯罪対策課
公式LINEアカウントで
情報配信中！

@387ojopi