アイホン株式会社　＞　脆弱性に関する情報

テナントビル用インターホン集合玄関機「GT-DMB-N」・「GT-DMB」
攻撃を受けた際に、本製品内の設定情報の流出や機能の一部が失われるなどの脆弱性

公開日　2022 年 11 月 10 日
最終更新日　2022 年 11 月 10 日

■概要
GT システム集合玄関機「GT-DMB-N」・「GT-DMB」に脆弱性が存在することが判明しました。
この脆弱性を悪用された場合、悪意のある第三者の攻撃により、本製品内の設定情報の不正な取得や改ざんによって、共用部玄関のオートロックの解錠が不正になされる可能性があります。

なお、当攻撃は極めて専門性の高い技術が必要であることから、本製品の発売後、当攻撃を要因とした被害発生の報告は一切ございません。

■JPCERT/CC による脆弱性分析結果
CVSS v3　CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N 基本値: 4.3
CVSS v2　AV:A/AC:M/Au:N/C:P/I:N/A:N 基本値: 2.9

■該当製品の確認方法
影響を受ける製品の品番は以下となります
製品品番　「GT-DMB-N」・「GT-DMB」
該当バージョン　Ver3.00 以前の全てのバージョン

ご使用されているバージョン番号の確認方法は以下の通りです。（管理者等による確認方法）
1. GT-DMB の「＃」ボタンを押し、ID コード入力画面を表示します。
2. ID コード入力画面で、施工者 ID コード（管理会社などに確認してください）を 2 回入力します。
操作を間違った場合は、「×」キーで待受け画面に戻り、前手順から再度やり直してください。
3. 設定画面が表示され、右上のバージョン表示を確認します。

■脆弱性の説明
専門的な技術を用いた攻撃を受けた際に、本製品内の設定情報の流出や製品機能の一部が失われるなどの脆弱性になります。

■脆弱性がもたらす脅威
本製品内の設定情報の不正な取得や改ざんによって、共用部玄関のオートロックの解錠が不正になされる可能性があります。

■対策方法
対策ファームウェア適用済み製品を使用する。

2021 年 12 月 7 日以降に出荷した製品は対策ファームウェアを適用済みです。
2021 年 12 月 7 日より前に出荷された製品への対応については、当社へ問い合わせてください。

■回避策
　なし。（上記対策方法のみが有効回避策となります）

■関連情報
　JVN#75437943　アイホン製インターホンシステムにおける情報漏えいの脆弱性
　CVE-2022-40903
　ホームページへの掲載：https://www.aiphone.co.jp/customer/20221110.html

■謝辞
　この脆弱性情報は、次の方が開発者に報告し、製品利用者への周知を目的に、開発者が IPA に報告し、JPCERT/CC が開発者との調整を行いました。
報告者: PROMON Cameron Palmer 氏

■更新履歴
　2022.11.10　脆弱性情報ページを公開しました。
　2022.11.10　参考情報「JVN#75437943」を追加しました

■連絡先
　アイホンお客様相談センター
固定電話からお掛けの場合：0120-141-092 （フリーダイヤル）
携帯電話からお掛けの場合：0565-43-1390
お問い合わせフォームからご連絡いただくには、以下の「製品に関するお問い合わせフォーム」よりご連絡ください。
製品に関するお問い合わせフォーム