お客様　各位

2019年 5月31日
株式会社ミントウェーブ

弊社 Windows Embedded 搭載シンクライアント端末のセキュリティ対応について

拝啓　貴社益々ご清栄のこととお慶び申し上げます。平素は格別のご高配を賜り、厚く御礼申し上げます。

2019年5月15日、マイクロソフト株式会社より、リモートデスクトップサービスにおける脆弱性 CVE-2019-0708 についてのセキュリティ更新プログラム（緊急）が公開されました。

参考URL1：CVE-2019-0708 | リモート デスクトップ サービスのリモートでコードが実行される脆弱性
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2019-0708

下記をご確認いただくとともに、対応頂けますようお願い申し上げます。

敬具

ー記ー

1. 対象製品（Windows Embedded 搭載モデルのみ）

表1に記す機種において、脆弱性が存在します。

表 1　Windows Embedded 搭載端末一覧

機種名	搭載 OS 名	販売終了日
MiNT-ACC F2-80	Windows XP Embedded SP2	2013/03/31
MiNT-ACC BX-80		2010/08/31
MiNT-ACC cute-40U/e		2011/03/31
MiNT-ACC cute-40Ub/e		2011/12/31
MiNT-ACC Note HV/E		2014/12/31
MiNT-ACC Note EA	Windows Embedded Standard 2009	2016/01/31
MiNT-ACC Note EB		2014/01/31
SunLite FA		販売中
MiNT-ACC E210	Windows Embedded Standard 7	販売中

その他、カスタマイズモデルについては、別途お問い合わせください。

2. リスク軽減策

マイクロソフト株式会社が紹介しているリスク軽減策は、次の通りです。

システムのプロパティ画面にて、（対象製品への）RDP接続を受け付けないように設定する。
（参考URL1［問題を緩和する要素］、参考URL2［6.よくあるQA集 の4項］に記載）

（補足）
・対象製品へのRDP接続は、工場出荷時は「受け付けない」設定となっております。
・対象製品へのRDP接続を「許可する（受け付ける）」設定に変更されている場合
① 運用上不要 ⇒RDP接続を「受け付けない」設定に変更してください。
（参考URL2の 6.よくあるQA集 の4項 を参照ください）
② 運用上必要 ⇒この脆弱性に対するセキュリティ更新プログラムを適用してください。

参考URL2：CVE-2019-0708 (Remote Desktop Service の脆弱性) について
https://social.technet.microsoft.com/Forums/ja-JP/ba328ae3-5cf5-4cf0-ac4e-6bef28c76883/cve20190708-remote-desktop-service-1239833030243692461 5?forum=Wcsupportja

3. お問い合わせ窓口

セキュリティ更新プログラムの適用方法・対象機器に関するお問い合わせは、機種名・S/Nをご確認の上、以下窓口にお願い申し上げます。

株式会社ミントウェーブ　保守・修理センター
e-mail:service@mintwave.co.jp

以上