2018 年 5 月 7 日

Plaza-i 利用ユーザ各位

株式会社ビジネス・アソシエイツ
技術サポート部

2018年5月更新プログラム適応によるRDS接続への影響

拝啓　貴社ますますご清祥のこととお喜び申し上げます。平素は格別のご高配を賜り、厚くお礼申し上げます。

マイクロソフト社より発表されましたCredSSP と呼ばれる認証プロトコルの脆弱性に関する対策に関しまして、リモートデスクトップ接続（以下 RDS）について問題が生じる可能性があるためご案内させていただきます。S
注意頂きたい点を下記に記載致しますのでご確認下さい。

敬具

記

CredSSP の脆弱性情報 CVE-2018-0886 対策のためリリースされた 3 月の更新プログラムを基として、新たに 5 月にリリースされる更新プログラムにて更にセキュリティレベルが上がります。
全てのコンピューターに更新プログラムが適用済みであれば問題はありませんが、3 月以降の更新プログラムがリモートデスクトップ接続先に適用されていない状態で、接続元に 5 月の更新が適用されると既定ではリモートデスクトップ接続ができなくなります。

具体的には下記ケースにてリモートデスクトップ接続先で問題が生じます。

・リモートデスクトップ接続先 【Plaza-i アプリケーションサーバもしくは DB サーバ】(RD 接続ブローカーを含む) が 3 月の更新プログラム未適用
・リモートデスクトップ接続元【Plaza-i 利用 RDP クライアント PC】が 5 月の更新プログラム適用済み

解決策と致しまして
リモートデスクトップ接続先【Plaza-iアプリケーションサーバもしくはDBサーバ】に CVE-2018-0886 の 3 月以降の更新プログラムを適用頂く必要が御座います。
弊社サポートで DB サーバに対し RDS 接続をしているユーザ様におかれましても、ご対応の程お願い致します。
自社環境で RDS を利用した Plaza-i 運用をしているか不明である場合や特別な事情で更新アップデート適応ができない場合などは、弊社までご相談ください。
セキュリティリスクが高まりますが、一時的な回避策をご案内致します。

参考 URL（２０１８年５月７日現在）
https://blogs.technet.microsoft.com/askcorejp/2018/05/02/2018-05-rollup-credssp-rdp/

以上

【本件に関するお問い合わせ】
株式会社ビジネス・アソシエイツ

技術サポート部　　電話番号 03-5495-9961　(内線73)　E-mail：　bassa@ba-net.co.jp