A890101KU

平成 20 年9月 1 日

お客様各位

NVC NETWORK VALUE COMPONENTS

株式会社ネットワークバリューコンポネンツ

DNSキャッシュ・ポイゾニング攻撃に対する脆弱性のお知らせ

拝啓、貴社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。

2008 年 8 月現在、ジュニパーネットワークスの NetScreen シリーズ及び SSG シリーズに搭載されている ScreenOS に重要な脆弱性がある旨、メーカより報告がございました。この勧告では既存システムの保護の観点より脆弱性の詳細については記述致しませんが、現在下記の情報が報告されております。

この DNS キャッシュ・ポインゾニングにより、ハッカーが DNS サーバの情報が書き換えるという攻撃を行い、正規サイトにアクセスしようとしたユーザが悪意あるサイトに誘導されてしまう可能性がございます。また、本脆弱性により、下記対象 ScreenOS バージョンを使用している全ての機器が影響されます。

この問題を回避するために、対象となるユーザ様は直ちにパッチ版ソフトウェアバージョンにアップグレードすることを強く推奨致します。

日頃のご愛顧に厚く御礼申し上げますと共に、今後とも弊社及び弊社製品のご愛顧を賜りますよう、お願い申し上げます。

敬具

記

1. 対象機器
   - SSG5, SSG20, SSG140, SSG320M/350M, SSG520M/550M
   - NS5XP, NS5XT, NS5GT, NS25, NS50, NS204/208, NS,500
   - ISG1000, ISG2000
   - NS5200/NS5400
2. 対象ソフトウェア
   - Screen OS5.1.0 以降 Screen OS5.4.0r10 以前にリリースされたすべてのバージョン
   - ScreenOS6.0.0 以降 6.0.0r5a 以前にリリースされたすべてのバージョン
3. 対象ユーザ
   - 上記対象ソフトウェアを利用し、かつ Proxy DNS を Enable にしている全てのユーザ
     （初期設定では Disable の設定となっております。有効にされていない場合は問題ございません。）
4. 対策
   - 下記二通りの対応方法がございます。
     - 修正版 OS バージョンへアップグレードする。
     - DNS Proxy の設定を無効設定に戻す。
5. 修正版 OS バージョン
   - ScreenOS6.0.0r6
   - ScreenOS5.4.0r10
6. 修正版 OS バージョンの取得方法

   下記弊社ユーザサポートページの OS ダウンロードページへアクセスしてください。

   ソフトウェアのダウンロードには ID/Password が必要になります。

   http://gold.nvc.co.jp/supports/Juniper/

＜重要＞

※ 冗長構成をご利用の御客様で RMA によって機器を交換した経緯のあるお客様は OS を統一していただきますようお願い致します。

※ 弊社より SSG300M シリーズをご購入いただいているお客様に対しましては以前より FAN 稼動による脆弱性のパッチバージョンを搭載させていただいておりましたが、この FAN 稼動による問題も、上記推奨 OS バージョン(OS6.0.0r6)にて修正されております。SSG320M または 350M をご利用になり、かつ DNS ポイゾニングの対象となるお客様は、速やかに OS6.0.0r6 へのアップグレードを徹底していただけますようお願いいたします。

※ 機種毎にパッチバージョンが異なります。上記ユーザサポートサイト、推奨 OS バージョン一覧よりご利用の機器に該当する推奨バージョンを確認していただくか、弊社サポート窓口までお問い合わせください。お問い合わせの際はご利用の機器、シリアル番号をご提示いただけますようお願いいたします。

※ 上記 OS バージョン以外の OS には本脆弱性は内在いたしません。

なお、本件につきましてのお問い合わせは、下記宛にお願い致します。

お客様問い合わせ窓口:

株式会社ネットワークバリューコンポネンツ　プロダクトマーケティング
電話番号:03-5783－1500
受付期間:2008 年 9 月 1 日(月) - 2008 年 9 月 12 日(金)
受付時間:午前 9:00 - 午後 6:00 (土日祭日は休止させていただきます)

上記受付期間終了後は、下記のメールアドレスにて、お客様からのお問い合わせを受け付けいたします。
sales@nvc.co.jp

以上