A8101001KU

平成 20 年 10 月 10 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

クロスサイトスクリプティング(XSS)に関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 10 月 6 日 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。

この問題により、不正な Management アクセスを行った際に記録される Login Failure のイベント・ログを、システムの管理者が WebUI を用いて表示した場、意図しないリモート Script が実行されてしまう可能性がございます。この問題は、Login Failure のイベント・ログを WebUI 上で表示させた場合に、Screen OS が不正な文字列を「リモート・サイトからスクリプト実行する」という命令に書き換えてしまうことにより発生いたします。

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修正済みの OS バージョンにアップグレードしていただく事を強く推奨いたします。また、即時のアップグレードが不可能な場合は下記ワークアラウンドを実施していただきますようお願い致します。

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
   - すべての SSG シリーズ
   - すべての NS シリーズ
   - すべての ISG シリーズ
2. 対象ソフトウェア
   - OS5.0.0-OS5.2.0 (技術サポート終了のため影響の有無を確認中)
   - OS5.3.0 すべてのリビジョン (影響あり)
   - OS5.4.0r1-OS5.4.0r9 (影響あり)
   - OS6.0.0r1-OS6.0.0r5, OS6.0.0r5a (影響あり)
   - OS6.1.0r1(影響あり。弊社では未リリースのため対象外になります)
3. 回避策
   - 修正版 OS へのアップグレード
   - 設定によるワークアラウンド
     - WebUI を Disable とする (unset interface xxxx manage web)
       - ※ https をご利用の場合は https の WebUI も Disable にする必要がございます。
         (unset interface xxxx manage ssl)
     - 信頼できる端末からのみ Management アクセスを可能とする (set admin manager-ip a.b.c.d)

4. 修正済 OS バージョン

- NetScreen 5XT をご利用のお客様

  OS5.3 のリビジョンが近日リリースとなります。

  それまでは下記ワークアラウンドを実施いただきますようお願い致します。

- NetScreen 5XT 以外の機種をご利用のお客様

  弊社サポートサイトの機種別の推奨 OS バージョンをご確認の上、下記どちらかのバージョンへアップグレードをお願いいたします。また、アップグレードが即時不可能である場合は上記ワークアラウンドを実施していただきますようお願い致します。

  - ScreenOS5.4.0r10
  - ScreenOS6.0.0r6

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

5. 修正版 OS バージョンの確認･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/

   OS に関する情報（サポート終了、脆弱性、販売終了のお知らせ）も上記サイトよりご確認頂けます。

＜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。

※ 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になっている機器、シリアル番号をご提供ください。

※ 上記ハードウェア、OS の組み合わせ以外の製品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：03-5783－1502
Email でのお問い合わせ：sales@nvc.co.jp
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）

今後、脆弱性やサポート終了などの技術情報をメール配信でご希望の方は、お手数ですが下記メールアドレスに必要情報を含めご返信ください。ご担当者の変更、本件の様なお知らせ廃止のご要望につきましても同様の方法でご連絡ください。

必要情報：貴社名
ご担当者部署
ご担当者お名前
ご利用の機種名
ご担当者メールアドレス

宛先：register@nvc.co.jp

以上