平成 27年 12 月 24 日

【追記平成 28 年 1 月 7 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

Juniper ScreenOS の脆弱性について

拝啓、貴社いよいよ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。

さて、この度 Juniper 製品の ScreenOS 搭載機にて脆弱性[Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)]の報告がありましたのでご報告させて頂きます。

敬具

記

1. 対象

・ScreenOS6.2.0r15 から 6.2.0r18

・ScreenOS6.3.0r12 から 6.3.0r20

※上記以外の ScreenOS バージョン及び他製品は影響を受けません。

2. 脆弱性の内容

Juniper 社 ScreenOS につきまして、セキュリティ問題が発見されました。

[CVE-2015-7755]

この脆弱性により、機器に対する不正な管理者アクセスが実施される可能性があります。

ログ出力例）

・通常ユーザ：username1

2015-12-17 09:00:00 system warn 00515 Admin user username1 has logged on via SSH from …..

2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin user ‘username1’ at host …

・不正アクセスに使用されているユーザ：username2

2015-12-17 09:00:00 system warn 00515 Admin user system has logged on via SSH from …..

2015-12-17 09:00:00 system warn 00528 SSH: Password authentication successful for admin user ‘username2’ at host …

熟練攻撃者の場合、不正アクセスの痕跡が巧妙に消去されている可能性があることにご留意ください。

[CVE-2015-7756]※追記

CVE-2015-7756 の脆弱性により、VPN 通信の復号化が可能となります。

知識を持った攻撃者が通信内容を解読可能となる問題です。

これは、1 件目(CVE-2015-7755)のものとは独立した問題となります。

この脆弱性が使用されたかどうかを確認する方法はありません。

3. 対応策

解決方法：修正 OS の適用・アップグレードを実施頂きますようお願い致します。

他の回避策がございませんので、対象外ソフトウェアバージョンへのアップグレードの実施をお願いいたします。

・ScreenOS6.2.0r19 および、それ以降のバージョン

・ScreenOS6.3.0r21 および、それ以降のバージョン

また、以下バージョンも本件の修正がなされております。

・ScreenOS6.3.0r12b, 6.3.0r13b, 6.3.0r14b, 6.3.0r15b, 6.3.0r16b ScreenOS6.3.0r17b, 6.3.0r18b, 6.3.0r19b

その他、本件に関しますお問い合わせ等につきましては弊社担当営業、もしくは下記までお問い合わせいただきますようお願い申し上げます。

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 マーケティング

電話番号：03-5714－2042

メール：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）