NVC NETWORK VALUE COMPONENTS

2003 年 7 月 31 日

お客様各位

株式会社ネットワークバリューコンポネンツ

DoS 攻撃に関する脆弱性への対応について

NetScreen 製品の DoS 攻撃に関する脆弱性により、ネットワーク機器がクラッシュまたはリブートを引き起こす問題が発表されております。
本問題に対する NetScreen 製品に関するコメントをご案内いたします。

記

危険度：中

1. 対象機器
   NetScreen IDP、ScreenOS 4.0.1r1 から 4.0.1r6、4.0.3r1、4.0.3r2 をインストールしている NetScreen Firewall/VPN 製品

2. NetScreen が受ける影響
   悪意のあるユーザーが TCP window option が変更されたマシンから NetScreen 管理 IP に対して接続を行った場合、NetScreen 製品がクラッシュ又はリブートを引き起こす可能性があります。

3. 推奨する対策
   NetScreen では本インシデントに対し以下のいずれかの対策を推奨しています。
   - 対策 1:管理ポートへのアクセスを制限
     製品へアクセス可能な端末を制限してください。
     CLI から以下のコマンドで制限ができます。
     ″set admin manager-ip ″
   - 対策 2:NetScreen 管理ポートの閉鎖
     NetScreen 管理ポートをすべて閉じてください。
     WebUI または CLI から全ての Interface の Management を OFF にしてください。
   - 対策 3:修正バージョンへのアップグレード
     本件に関して、問題が修正されたパッチがリリースされております。
     修正済み OS：4.0.3r3/4.0.1r7 以降

以　上