NVC NETWORK VALUE COMPONENTS

2002 年 2 月 19 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

SNMP に関するセキュリティ・ホールへの弊社取扱製品の対応について

記

米 CERT/CC より報告された CA-2002-03、 SNMP に関するセキュリティ・ホールへの対応を報告します。
SNMPv1 を実装した機器の多くに、脆弱性が報告されています。
各社の対応をそれぞれ列挙します。

- Riverstone 社
- Enterasys 社
- Alteon WebSystems 社
- NetScreen 社

Riverstone 社

Riverstone では、対策を施したパッチバージョンのファームウェア ROS8.0.3.3 を近日中にリリースし、推奨 OS とさせていただきます。また今後ファームウェアに関しましては、全て本対応プログラムを適用した OS にてリリースいたします。
推奨 OS につきましては User's Page にてご確認をお願い申し上げます。
http://www.riverstonenet.com/

Enterasys 社

Enterasys では、対策を施したパッチバージョンを近日中にリリースいたします。
http://www.enterasys.com/support/

Alteon WebSystems 社

Alteon WebSystems では、対策を近日中にリリースいたします。

NetScreen 社

SNMPv1 のセキュリティ・ホールに関して NetScreen より緊急報告とそれに対してのメンテナンスパッチがリリースされました。

解決方法

各 Interface Management 設定において必要の無い SNMP agent を無効にしておきます。
SNMP を使用して管理をする場合、VPN 経由で情報を流すことをお勧めします。
可能であれば Default で使用されている、UDP Port 番号を使用しないことをお勧めします。
SNMP で管理可能な送信元 IP Address を指定しておきます。(最大 8IP Address まで) NetScreen 自体 SNMP を利用して Operaion はできません。全ての機器において MIB 変数は Read-Only になっています。

各 ScreenOS において CERT と OUSPG でのテストで影響の受けた物に関しては、下記のメンテナンスパッチを当てる事により、回避ができます。
緊急に ScreenOS に対して、下記のパッチを当てる事をお勧めいたします。
http://www.netscreen.com/support/snmp.html　（英文）

一般的に報告されているセキュリティ・ホールの報告の内容（IT PRO ニュース抜粋)

SNMP のセキュリティ・ホールを悪用すると，コンピュータやネットワーク機器のサービスを中断あるいは停止させることができる。任意のコードを実行されて，コンピュータなどを乗っ取られる恐れさえある。
対策は修正パッチの適用や不要な SNMP サービスの停止，外部からの SNMP アクセスの禁止など。ネットワークに接続された多くの機器が影響を受け，既に攻撃が報告されている。ネットワーク管理者などは早急に対策を施す必要がある。

以　上