NVC NETWORK VALUE COMPONENTS

2002 年 3 月 11 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。

- Inktomi 社
- Alteon WebSystems 社

Inktomi 社

米国 CERT/CC より報告されたネットワーク機器に対する SNMPv1 のセキュリティに関する脆弱性について Inktomi 社の対応についてご案内いたします。
TS/Media-IXT（5.2 より前のリリースバージョン全て）と Content Networking Platform（1.0）は脆弱性を含んでいます。速やかなバージョンアップをお願いします。

- 影響を受ける製品・バージョン
  下記製品・バージョンは脆弱性を含んでいます。

TS/Media-IXT	5.2 より前のリリースバージョン全て
Content Networking Platform	1.0

詳細
TS/Media-IXT には snmpdm というモジュールが入っており、このモジュールによって MRTG グラフに必要な情報などを SNMP を使用して取得しています。
このモジュールのバージョンが 15.3.1.7 より古ければ、脆弱性を含んでいます。
今回対象の TS/Media-IXT などには 15.3.1.7 より古いバージョンが使用されています。
snmpdm のバージョン一覧(脆弱性対策済みバージョン)
Supporting Versions

Irix	15.3.1.13
DEC (osf4)	15.3.1.13
HPUX (hpux11)	15.3.1.7
Linux	15.3.1.7
Sun Solaris	15.3.1.7
Windows	32 15.3.1.7

snmpdm のバージョン情報表示の方法
【UNIX】

```
cd `cat /etc/traffic_server`
cd bin
./snmpdm
```

【Windows】
TS のインストールディレクトリに移動し、
cd bin
./snmpdm.exe

- 対策
  snmpdm が該当バージョンであった場合、このモジュールに関してアップデートが必要になります(TS/Media-IXT 自体のアップデートではありません。)
- 手順
  1. snmpdm の最新バージョンを入手してください。
  2. TS/Media-IXT を停止させてください。
  3. snmpdm を最新バージョンと入れ替えてください。
  4. TS/Media-IXT を起動させてください。

メーカー推奨の方法は上記で、TS の停止を伴いますが、停止せずにアップデートする方法もございます。
詳しいアップデート方法やアップデートモジュールの入手に関しては、弊社にお問合せください。

Alteon WebSystems 社

Alteon 180e/184 and ACEdirector3/4 (WebOS) [Releases 10.0]、Alteon Switched FireWall (ASF)、Alteon Content Director は脆弱性を含んでいます。
対応ファームウエアに関しては 2002 年 3 月中旬に Software Fix のリリースを予定しております。リリース・提供方法に関しては再度周知させていただきます。

- 影響を受けない製品・バージョン
  下記製品・バージョンは脆弱性に対し確認が取れております。
  影響を受けない製品・バージョン
  Alteon 180e/184 and ACEdirector3/4 (WebOS)　Releases 8.x and 9.0
  Alteon iSD SSL Accelerator
  Alteon Content Manager (ACM)
  影響を受ける製品・バージョン
  Alteon 180e/184 and ACEdirector3/4 (WebOS)　Releases 10.0
  Alteon Switched FireWall (ASF)
  Alteon Content Director

2002 年 3 月中旬に Software Fix のリリースを予定しております。
詳細については、Nortel 社からの文書(英文) 1 2 を参照ください。
詳しいアップデート方法やアップデートモジュールの入手に関しては、弊社にお問合せください。

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