2005 年 4 月 19 日

お客様各位

セイコーインスツル株式会社
ネットワークシステム部

「TCP 実装の ICMP エラーメッセージの処理に関する脆弱性」について

拝啓、貴社益々ご清栄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、2005 年 4 月 12 日に発行された Security　Advisory について、弊社製品における本脆弱性の調査を行いましたので下記に報告いたします。
何卒ご査収くださいますよう宜しくお願い致します。

敬　具

記

１．Security Advisory について

下記の Security Advisory「TCP 実装の ICMP エラーメッセージの処理に関する脆弱性」が発行されました。ICMP を利用した TCP プロトコルに対する様々な攻撃法が存在します。

http://www.niscc.gov.uk/niscc/docs/al-20050412-00308.html?lang=en
http://www.kb.cert.org/vuls/id/222750

上記の公開情報には、以下の３つの脆弱性が存在すると記載されています。

(1) ICMP Destination Unreachable packet (ICMP TYPE=3)
(2) Path MTU discovery
(3) ICMP Source Quench

２．脆弱性の影響度

本脆弱性は弊社 NS シリーズが終端している TCP コネクション（管理用の telnet や FTP セッション）に関連するもので、本脆弱性のアタックを受けても、ルータやスイッチとしてのフォワーディング動作に影響はございません。
NS シリーズは、上記１．の３つの脆弱性の内 (3)のみに該当しますが、このアタックを受けた場合には NS が終端している telnet などの TCP セッションの送信が一時的に絞られるという影響があります。攻撃された TCP ポートに対する NS からの送信が絞られる以外に、悪影響はございません。（詳細は下記をご参照ください）

	型番	ICMP Destination Unreachable packet	Path MTU discovery	ICMP Source Quench
EXAtrax	NS-61XX	影響なし	影響なし	影響あり
BlueBrick	NS-272X NS-273X	影響なし	影響なし	影響あり
RAS	NS-4200 NS-2484 NS-2610	影響なし	影響なし	影響あり
CS	NS-2234 NS-2232	影響なし	影響なし	影響あり

(1) ICMP Destination Unreachable packet (ICMP TYPE=3)

本件は、すでに ESTABLISH になっている TCP のセッションに対して、ICMP の Destination Unreachable を受け取ると、ESTABLISH になっているセッションを開放する脆弱性です。

弊社 NS シリーズは、TCP が SYN_SENT 状態の時のみ、"Destination Unreachable"を受信すると RESET を送信します。それ以外の状態では、このパケットは無視されますので、本アタックに対する NS シリーズへの影響はございません。

(2) Path MTU discovery

本件は、Path MTU discovery を使っているときに、ICMP の Destination Unreachable の"fragmentation need and DF set"を受け取ると、MTU を小さくする脆弱性です

弊社 NS シリーズは、Path MTU discovery 機能はサポートしておりません。"ICMP Destination Unreachable(ICMP TYPE=3)" の "Fragmentation Needed and DF set (Code=4)"を受信しても、本アタックに対する NS シリーズへの影響はございません。

(3) ICMP Source Quench

本件は、TCP セッションに対して ICMP の Source Quench を受け取ると、送信を絞る脆弱性です。

弊社 NS シリーズは、ICMP Source Quench を受信すると、TCP はそのコネクションの送信を抑制しますので、この脆弱性に該当致します。
但し、本装置がこのアタックを受けたとしても、対象となる TCP は、本装置の telnetd やバージョンアップ用のサーバであり、管理用の telnet の送信が絞られたり、バージョンアップ作業が遅くなるなどの事象は発生しても、NS 自身の CPU 負荷が上がったりすることはありませんので、実質的な影響は低いと思われます。

３．ICMP Source Quench の対策について

本脆弱性は、成りすましされ、さらに ICMP Source Quench を利用した攻撃を受けた場合に影響があります。影響を軽減させるために、アクセスリスト（本装置の telnetd やバージョンアップ用のサーバにアクセスできるアドレスを制限する）を定義したり、管理 IP を独立させるなどの対策をお願いいたします。

抜本的な対策として、ICMP Source Quench に応答しないように、弊社ではシステムソフトウェアの修正を予定しております。本対策を反映させた各製品のシステムソフトウェアは、各製品のバージョンアップのスケジュールに合わせて提供させていただきます。

以上