ソフトウェア製品セキュリティ情報
Software Vulnerability Information

ソフトウェア事業部 (Software Division)

トップ

What's New

お知らせ

御参考（警告情報など）

ソフトウェア製品セキュリティ情報

セキュリティ対応機関へのリンク

お問い合わせ

soft-security
@itg.hitachi.co.jp

2005.05.23更新

JP1/Cm2/Network Node Manager におけるDoS脆弱性

- 影響がある製品

対策	製品名	適用ＯＳ	更新日
HS05-008-01	JP1/Cm2/Network Node Manager Enterprise JP1/Cm2/Network Node Manager 250 JP1/Cm2/Network Node Manager	HP-UX,Windows, Solaris	2005.05.23

- 問題の説明

上記の製品において、サービス拒否の脆弱性が存在することが判明しました。この脆弱性を利用した悪意のある第三者からの攻撃により、上記の製品がサービス不能に陥る可能性があります。

更新履歴 ：

- 2005.05.23 : 対策ページを更新しました。
- 2005.04.26 : このセキュリティ情報ページを新規作成および発信しました。

- 弊社では，セキュリティ対応に関して正確な情報を提供するよう努力しておりますが，セキュリティ問題に関する情報は変化しており，当ホームページで記載している内容を予告なく変更することがありますので，あらかじめご了承ください。情報ご参照の際には，常に最新の情報をご確認いただくようお願いします。
- 当ホームページに記載されている製品には，他社開発製品が含まれております。これらのセキュリティ情報については他社から提供，または公開された情報を基にしております。弊社では，情報の正確性および完全性について注意を払っておりますが，開発元の状況変化に伴い，当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ

トップ

What's New

お知らせ

御参考（警告情報など）

ソフトウェア製品セキュリティ情報

セキュリティ対応機関へのリンク

お問い合わせ
soft-security
@itg.hitachi.co.jp

個人情報保護ポリシーにご同意頂ける場合のみ、上記アドレスをご利用下さい。ご同意頂けない場合には、お問い合わせに回答できない場合があります。
なお、入力頂いた個人情報は本ポリシーに従って適切に管理し、問合せ対応のためにのみ使用します。第三者への個人情報の提供、預託、開示は法令に基づく場合を除いて行いません。
お問い合わせへの回答後、個人情報は当社が責任を持って適切に廃棄いたします。

日立および他社の商品名称に関する記述

2005.05.23更新

HS05-008;

JP1/Cm2/Network Node Manager におけるDoS脆弱性

JP1/Cm2/Network Node Manager におけるDoS脆弱性の対策

JP1/Cm2/Network Node Manager (NNM)において、悪意のある第三者から、NNM のプロセスが使用しているポートに不正なデータが送信された場合に，そのポートを使用しているプロセスが異常終了する、またはCPUを占有し、NNMがサービス不能に陥る可能性があります。サービス不能となった場合は、NNMのサービスを再起動させる必要があります。
下記に示すバージョンについて対策版をご提供いたします。この対策版へのバージョンアップをお願いします。

[影響範囲]

NNM バージョン07-10については本脆弱性の影響を受けません。
下表に記載されていない旧バージョンについては、本脆弱性の影響を受けますので、以下の[対策版の提供]に記載されている後継製品に移行いただ

くか、[暫定回避方法]に示す回避策による対応をお願いいたします。

[対策版の提供]

製品名	形名	対象バージョン	適用ＯＳ	吸収バージョン	提供時期	更新日
JP1/Cm2/Network Node Manager Enterprise	P-1B42-6161	06-00～06-51-/A	HP-UX	06-71-/C (注1)	2004.12.03	2005.04.26
		06-71～06-71-/B		06-71-/C	2004.12.03	2005.04.26
	P-2442-6164	06-00～06-51-/B	Windows	06-71-/C (注1)	2004.12.03	2005.04.26
		06-71～06-71-/B		06-71-/C	2004.12.03	2005.04.26
	P-9D42-6161	06-00～06-51-/B	Solaris	06-71-/C (注1)	2004.12.03	2005.04.26
		06-71～06-71-/B		06-71-/C	2004.12.03	2005.04.26
JP1/Cm2/Network Node Manager 250	P-1B42-6261	06-00～06-51-/A	HP-UX	06-71-/C (注1)	2004.12.03	2005.04.26
		06-71～06-71-/B		06-71-/C	2004.12.03	2005.04.26
	P-2442-6264	06-00～06-51-/B	Windows	06-71-/C (注1)	2004.12.03	2005.04.26
		06-71～06-71-/B		06-71-/C	2004.12.03	2005.04.26
	P-9D42-6261	06-00～06-51-/B	Solaris	06-71-/C (注1)	2004.12.03	2005.04.26
		06-71～06-71-/B		06-71-/C	2004.12.03	2005.04.26
JP1/Cm2/Network Node Manager	P-1B42-6271	07-00～07-00-/A	HP-UX	07-01-/B (注1)	2005.01.11	2005.04.26
		07-01～07-01-/A		07-01-/B	2005.01.11	2005.04.26
	P-2442-6274	07-00～07-00-/A	Windows	07-01-/B (注1)	2005.01.11	2005.04.26
		07-01～07-01-/A		07-01-/B	2005.01.11	2005.04.26
	P-9D42-6271	07-00～07-00-/A	Solaris	07-01-/B (注1)	2005.01.11	2005.04.26
		07-01～07-01-/A		07-01-/B	2005.01.11	2005.04.26

(注1) 本製品は、リビジョンアップをお願いいたします。

NNMのリビジョンアップにより、NNM上で動作する連携製品についても、バージョンアップもしくはリビジョンアップが必要となる場合があります。NNMと連携する製品がどのバージョンのNNMに対応しているかについては、各製品のソフトウェア添付資料やReadme等のドキュメントをご参照ください。

- サポートサービスをご契約されているお客様

  サポートサービスの改良版の提供についてのホームページをご参照いただき，ホームページでご案内している手順にしたがって，対策版をご入手ください。

- サポートサービスをご契約されていないお客様

  JP1/Cm2/Network Node Managerに関しては，ライセンス管理を適切に行なう必要があるため，お手数ですが，こちら より提供をご依頼ください。
  上表に記載されていない旧バージョンについては、別途ご相談下さい。

[暫定回避方法]

この脆弱性に対して下記暫定回避策があります。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。
NNMで使用しているTCPポート宛の通信を信頼できる相手のみに限定するよう、ファイアウォールまたはルータにフィルタリング設定を行ってください。

更新履歴 ：

- 2005.05.23 : 冒頭の説明内容に関して情報を追記しました。
- 2005.04.26 : JP1/Cm2/Network Node ManagerにおけるDoS脆弱性の情報を公開しました。

- 弊社では，セキュリティ対応に関して正確な情報を提供するよう努力しておりますが，セキュリティ問題に関する情報は変化しており，当ホームページで記載している内容を予告なく変更することがありますので，あらかじめご了承ください。情報ご参照の際には，常に最新の情報をご確認いただくようお願いします。
- 当ホームページに記載されている製品には，他社開発製品が含まれております。これらのセキュリティ情報については他社から提供，または公開された情報を基にしております。弊社では，情報の正確性および完全性について注意を払っておりますが，開発元の状況変化に伴い，当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ