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)

2006.07.20更新

JP1/Cm2/Network Node Manager のWeb連携機能における複数の脆弱性

- 影響がある製品

対策	製品名	適用ＯＳ	更新日
HS05-018-01	Cm2/Network Node Manager Enterprise Cm2/Network Node Manager Unlimited Cm2/Network Node Manager 250 JP1/Cm2/Network Node Manager Enterprise JP1/Cm2/Network Node Manager 250 JP1/Cm2/Network Node Manager	HP-UX, Windows, Solaris, HI-UX/WE2	2006.07.20

- 問題の説明

JP1/Cm2/Network Node ManagerのWeb連携機能に複数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、JP1/Cm2/Network Node Managerがサービス不能に陥ったり任意のコマンドが実行される可能性があります。

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

更新履歴 ：

- 2006.07.20 : 対策ページを更新しました。
- 2005.10.31 : 対策ページを更新しました。
- 2005.09.09 : 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

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

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

2006.07.20更新

HS05-018;

JP1/Cm2/Network Node Manager のWeb連携機能における複数の脆弱性

JP1/Cm2/Network Node Manager の対策

JP1/Cm2/Network Node Manager (以下NNMと略す)のWeb連携機能に複数の脆弱性が存在することが判明しました。悪意のある第三者からの攻撃により、以下の問題が発生する可能性があります。

(問題1) 不適切なHTTPリクエストにより、Web機能がサービス不能に陥る

(問題2) 不適切なHTTPリクエストにより、任意のコマンドが実行される

(問題3) Web認証機能が有効にならない

影響を受けるバージョンを下記に示しますので、[暫定回避方法]による回避、または対策版へのバージョンアップをお願いいたします。

[該当形名･バージョン]

影響を受けるバージョンを下記に示します。

製品名	形名	該当バー	適用OS	該当する問題 (注1)

		ジョン		(問題1)	(問題2)	(問題3)
Cm2/Network Node Manager Enterprise	P-1B42-5111	05-00～05-00-/C	HP-UX	○	×	×
	P-1642-511	05-00	HI-UX/WE2	○	×	×
Cm2/Network Node Manager Unlimited	P-2442-5194	05-00～05-00-/A	Windows	○	×	×
Cm2/Network Node Manager 250	P-1B42-5211	05-00～05-00-/C	HP-UX	○	×	×
	P-2442-5294	05-00～05-00-/A	Windows	○	×	×
	P-1642-521	05-00	HI-UX/WE2	○	×	×
JP1/Cm2/Network Node Manager Enterprise	P-1B42-6111	05-20～05-20-/E	HP-UX	○	○	×
	P-1B42-6161	06-00～06-50-/A		○	○	×
		06-51～06-71-/C		○	○	○
	P-2442-6194	05-20～05-20-/F	Windows	○	○	×
	P-2442-6164	06-00～06-50-/A		○	○	×
		06-51～06-71-/D		○	○	○
	P-9D42-6111	05-20～05-20-/E	Solaris	○	○	×
	P-9D42-6161	06-00～06-50-/A		○	○	×
		06-51～06-71-/C		○	○	○
	P-1B42-6211	05-20～05-20-/E		○	○	×
		06-00～				

JP1/Cm2/Network Node Manager 250	P-1B42-6261	06-50-/A	HP-UX	○	○	×
		06-51～06-71-/C		○	○	○
	P-2442-6294	05-20～05-20-/F	Windows	○	○	×
	P-2442-6264	06-00～06-50-/A		○	○	×
		06-51～06-71-/D		○	○	○
	P-9D42-6211	05-20～05-20-/E	Solaris	○	○	×
	P-9D42-6261	06-00～06-50-/A		○	○	×
		06-51～06-71-/C		○	○	○
JP1/Cm2/Network Node Manager	P-1B42-6271	07-00～07-10-02	HP-UX	○	○	○
		07-10-03		×	○	○
	P-2442-6274	07-00～07-10-02	Windows	○	○	○
		07-10-03		×	○	○
	P-9D42-6271	07-00～07-10-02	Solaris	○	○	○
		07-10-03		×	○	○

(注1) ○印は、セキュリティ問題が発生します。×印はセキュリティ問題が発生しません。

[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
	P-1B42-	06-00～	HP-UX	(注4)		2006.07.20

	6161	06-71-/C				
JP1/Cm2/Network Node Manager Enterprise	P-2442-6164	06-00～06-71-/D	Windows	(注4)		2006.07.20
	P-9D42-6161	06-00～06-71-/C	Solaris	(注4)		2006.07.20
JP1/Cm2/Network Node Manager 250	P-1B42-6261	06-00～06-71-/C	HP-UX	(注4)		2006.07.20
	P-2442-6264	06-00～06-71-/D	Windows	(注4)		2006.07.20
	P-9D42-6261	06-00～06-71-/C	Solaris	(注4)		2006.07.20
JP1/Cm2/Network Node Manager	P-1B42-6271	07-00～07-01-/B	HP-UX	07-10-04 (注2)	2005.10.21	2005.10.31
		07-10～07-10-03		07-10-04 (注3)	2005.10.21	2005.10.31
	P-2442-6274	07-00～07-01-/B	Windows	07-10-04 (注2)	2005.10.21	2005.10.31
		07-10～		07-10-04	2005.10.21	2005.10.31

		07-10-03		(注3)		
	P-9D42-6271	07-00～07-01-/B	Solaris	07-10-04 (注2)	2005.10.21	2005.10.31
		07-10～07-10-03		07-10-04 (注3)	2005.10.21	2005.10.31

(注2) 本製品はリビジョンアップをお願いします。
なお、NNMのバージョンアップ・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。

(注3) 対策版として提供するNNM 07-10-04(累積パッチ)は、NNM 07-10-02または07-10-03が前提となります。このため、NNM 07-10または07-10-01をご使用中のお客様は、07-10-04を適用する前に07-10-02を上書きインストールする必要があります。
また、NNM 07-10-02～07-10-03をご使用中のお客様で、CGIプログラムを任意のディレクトリに移動する暫定回避策を実施済みの場合、07-10-04をあてる前に、移動しておいたCGIプログラムを元のディレクトリに戻してください。

(注4) 本製品をお使いの方は、サポートサービス窓口へご相談願います。

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。

- 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。

[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。対策版が提供されるまでの間、以下の暫定回避策1.および2.を実施していただくようお願いいたします(2.については、バージョンが該当する場合のみ実施願います)。

1. (問題1)および(問題3)に対する暫定回避策

   NNMのWeb連携機能で使用するWebサーバーのTCPポート宛の通信を、信頼できるホストに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。

2. (問題2)に対する暫定回避策

   NNMが提供している下記CGIプログラムを、任意に作成した別ディレクトリに移動してください。

   - connectedNodes.ovpl (NNM 06-51以降のみ存在)
   - cdpView.ovpl (NNM 06-51以降のみ存在)
   - freeIPaddrs.ovpl (NNM 06-51以降のみ存在)
   - ecscmg.ovpl (NNM 05-20以降のみ存在)

   なお、上記 CGI プログラムは以下のディレクトリに存在します。

   - Windows版の場合

     "NNMインストールディレクトリ"¥www¥cgi-bin ディレクトリ
   - UNIX版の場合

     /opt/OV/www/cgi-bin ディレクトリ

   CGIプログラムの移動により、以下の機能が影響を受けます。

   - connectedNodes.ovpl

     GUI メニューから起動する「ポート/アドレス・マッピング」

メニューが使用できません。

- cdpView.ovpl

  CDP ビューが使用できません。

- freeIPaddrs.ovpl

  GUI メニューから起動する「未使用 IP アドレス」メニューが使用できません。

- ecscmg.ovpl

  イベント相関処理定義の設定が出来ません。

更新履歴 ：

- 2006.07.20 : [対策版の提供]の形名、P-1B42-6161、P-2442-6164、P-9D42-6161、P-1B42-6261、P-2442-6264、P-9D42-6261の吸収バージョン、提供時期を更新しました。
- 2005.10.31 : JP1/Cm2/Network Node Manager のWeb連携機能における複数の脆弱性の対策版の提供情報、暫定回避策に(問題1)、(問題2)、(問題3)の記述を追記しました。
- 2005.09.09 : JP1/Cm2/Network Node Manager のWeb連携機能における複数の脆弱性の情報を公開しました。

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