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)

2008.10.17更新

JP1製品におけるDoSの脆弱性

- 影響がある製品

対策	製品名	適用ＯＳ	更新日
HS06-007-01	JP1/PFM/SNMP System Observer - Report Feature, JP1/Server System Observer - Report Feature	Windows	2006.03.31
HS06-007-02	JP1/Automatic Job Management System 2 - Manager、 JP1/Automatic Job Management System 2 - Agent、 JP1/Automatic Job Management System 2 - Light Edition、 Job Management Partner 1/Automatic Job Management System 2 - Manager、 Job Management Partner 1/Automatic Job Management System 2 - Agent	Windows、HP-UX、Solaris、AIX、HP Tru64 UNIX、Linux、HI-UX/WE2	2006.09.29
	JP1/Performance Management - Manager、	Windows、HP-UX、	

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

HS06-007-03	JP1/Performance Management - View、 JP1/Performance Management - Agent	Solaris、AIX、 Linux	2008.02.04
HS06-007-04	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	Windows、Solaris、 HI-UX/WE2	2006.03.31
HS06-007-05	JP1/ServerConductor/Blade Server Manager, JP1/ServerConductor/Server Manager, ServerConductor/Blade Server Manager, ServerConductor/Server Manager, System Manager - Management Console	Windows	2006.03.31
HS06-007-06	JP1/File Access Control	Windows, HP-UX	2006.03.31
HS06-007-07	JP1/Security Integrated Manager, JP1/Security Integrated Manager - Runtime Library	Solaris	2006.03.31
HS06-007-08	JP1/ServerConductor/Deployment Manager Standard Edition, JP1/ServerConductor/Deployment Manager Enterprise Edition, ServerConductor/DeploymentManager	Windows	2006.05.31
HS06-007-09	JP1/Cm2/操作支援, JP1/Cm2/Operations Assist Manager, JP1/Cm2/Operations Assist SubManager, JP1/Cm2/SubManager,	Windows、HP-UX、 Solaris、AIX、 HI-UX/WE2	2008.10.17

	JP1/Cm2/Operations Assist Agent, JP1/Cm2/Extensible Agent		
HS06-007-10	JP1/Cm2/階層管理, JP1/Cm2/Hierarchical Agent, JP1/Cm2/SubManager	Windows	2006.09.14
HS06-007-11	JP1/Base, Job Management Partner 1/Base	Solaris	2007.07.06

- 問題の説明

  上記の製品において意図しない接続が行われた場合、または意図しないデータを受信した場合、サービスが停止する、またはサービスの応答が返らなくなる問題が判明しました。
  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 ：

- 2008.10.17 : HS06-007-09の対策ページを更新しました。
- 2008.02.04 : HS06-007-03の対策ページを更新しました。
- 2007.07.06 : HS06-007-11の対策ページを更新しました。
- 2007.02.15 : HS06-007-09の対策ページを更新しました。
- 2006.11.08 : HS06-007-11の対策ページを更新しました。
- 2006.09.29 : 影響がある製品、HS06-007-11を追加し、HS06-007-02,HS06-007-03を更新しました。
  HS06-007-02,HS06-007-03の対策ページを更新しました。
- 2006.09.14 : 影響がある製品、HS06-007-09,HS06-007-10を追加しました。
- 2006.05.31 : 影響がある製品、HS06-007-08を追加し、HS06-007-02を更新しました。
  HS06-007-02の対策ページを更新しました。

- 2006.03.31 : 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)

2006.03.31更新

HS06-007;

JP1製品におけるDoSの脆弱性

JP1/PFM/SNMP System Observer - Report Featureの対策

JP1/PFM/SNMP System Observer - Report Featureにおきまして，意図しないデータを受信した場合、JP1/PFM/SNMP System Observer - Report Feature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、JP1/PFM/SNMP System Observer - Report Featureサーバプロセスを再起動させるまたは、OSを再起動させる必要があります。

各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日
JP1/Server System Observer - Report	P-F2442-	06-71～06-71-/D		06-71-/E	2006.03.31	2006.03.31

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

Feature	6R641		Windows			
JP1/Server System Observer - Report Feature	P-F2442-6R671	06-71		(注1)		2006.03.31
JP1/PFM/SNMP System Observer - Report Feature	P-F242C-6T741	07-00～07-00-/A		07-00-/B	2006.02.16	2006.03.31
		07-10～07-10-/A		07-10-/B	2006.03.31	2006.03.31
		07-50		07-50-01	2006.02.06	2006.03.31
JP1/PFM/SNMP System Observer - Report Feature	P-F242C-6T771	07-00		(注1)		2006.03.31

(注1) 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。

- 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/PFM/SNMP System Observer - Report Feature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。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

JP1/PFM/SNMP System Observer - Report Featureで使用するポートの通信を信頼できるIPアドレスのみに限定するよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行なってください。

更新履歴 ：

- 2006.03.31 : JP1製品におけるDoSの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

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

2006.09.29更新

HS06-007;

JP1製品におけるDoSの脆弱性

JP1/Automatic Job Management System 2の対策

JP1/Automatic Job Management System 2(以下、JP1/AJS2と略す)におきまして、JP1/AJS2が使用している通信ポートから、意図しないデータを受信した場合、JP1/AJS2サービスが停止する場合があります。JP1/AJS2サービスを再起動までは、JP1/AJS2を使用したバッチジョブの運用ができない可能性があります。

各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日
	P-	07-50～07-50-05		07-50-06	2005.11.25	2006.03.31
		07-11～		07-11-08	2006.01.25	2006.03.31

P-2412-3K74	07-11-07	Windows (x86版)			
	07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
P-2812-3K74	07-50～07-50-05	Windows (IPF版)	07-50-06	2005.11.25	2006.03.31
	07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
P-2412-3K64	06-71～06-71-/M	Windows	06-71-/N	2006.02.16	2006.03.31
	06-51～06-51-/R		(注1)		2006.03.31
	06-00～06-00-N1		(注1)		2006.03.31
P-1B12-2771	07-50～07-50-05	HP-UX (PA-RISC版)	07-50-06	2005.11.25	2006.03.31
	07-11～07-11-07		07-11-08	2006.01.25	2006.03.31
	07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
P-1B12-2761	06-71～06-71-/M		06-71-/N	2006.02.16	2006.03.31
	06-51～06-51-/R		(注1)		2006.03.31
	06-00～06-00-/N		(注1)		2006.03.31
P-1J12-2771	07-50～07-50-05	HP-UX (IPF版)	07-50-06	2005.11.25	2006.03.31
	07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	07-50～07-50-05		07-50-06	2005.11.25	2006.03.31

JP1/Automatic Job Management System 2 - Manager	P-1M12-2771	07-11～07-11-07	AIX	07-11-08	2006.01.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
		07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
	P-9112-2761	06-71～06-71-/M		06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-/N		(注1)		2006.03.31
	P-9312-2771	07-50～07-50-05	Solaris	07-50-06	2005.11.25	2006.03.31
		07-11～07-11-07		07-11-08	2006.02.13	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
		07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
	P-9312-2761	06-71～06-71-/M		06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-/N		(注1)		2006.03.31
	P-9C12-2761	06-71～06-71-/M	HP Tru64 UNIX	06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-/N		(注1)		2006.03.31
		07-50～07-50-05	Red Hat Linux(7.1/7.2/7.3)	07-50-06	2005.11.25	2006.03.31

	P-9S12-2771	07-11～07-11-07	(x86版)Red Hat Enterprise Linux (AS 2.1/ES 2.1/WS 2.1) (x86版)Miracle Linux (x86版)	07-11-08	2006.01.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	P-9S12-3771	07-50～07-50-05	Red Hat Enterprise Linux (AS 3/ES 3)(x86版)	07-50-06	2005.11.25	2006.03.31
		07-11～07-11-07		07-11-08	2006.01.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	P-9V12-2771	07-50～07-50-05	Red Hat Enterprise Linux(AS 3)(IPF版)	07-50-06	2005.11.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	P-2412-3374	07-50～07-50-05	Windows (x86版)	07-50-06	2005.11.25	2006.03.31
		07-11～07-11-06		07-11-08	2006.01.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
		07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
	P-2812-3374	07-50～07-50-05	Windows (IPF版)	07-50-06	2005.11.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
		07-00		07-00-/G	2006.04.06	2006.05.31
	P-2412-3364	06-71～06-71-/L	Windows	06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-/N		(注1)		2006.03.31

	P-1B12-2971	07-50～07-50-05	HP-UX (PA-RISC版)	07-50-06	2005.11.25	2006.03.31
		07-11～07-11-06		07-11-08	2006.01.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
		07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
	P-1B12-2961	06-71～06-71-/L	HP-UX (PA-RISC版)	06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-/N		(注1)		2006.03.31
	P-1J12-2971	07-50～07-50-05	HP-UX (IPF版)	07-50-06	2005.11.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
		07-00		07-00-/G	2006.03.29	2006.05.31
	P-1M12-2971	07-50～07-50-05	AIX	07-50-06	2005.11.25	2006.03.31
		07-11～07-11-06		07-11-08	2006.01.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
		07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
	P-9112-2961	06-71～06-71-/L		06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-/N		(注1)		2006.03.31
JP1/Automatic Job Management System 2 - Agent		07-50～		07-50-06	2005.11.25	2006.03.31

P-9312-2971	07-50-05	Solaris			
	07-11～07-11-06		07-11-08	2006.02.13	2006.03.31
	07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
P-9312-2961	06-71～06-71-/L		06-71-/N	2006.02.16	2006.03.31
	06-51～06-51-/R		(注1)		2006.03.31
	06-00～06-00-/N		(注1)		2006.03.31
P-9C12-2971	07-11	HP Tru64 UNIX	07-11-09	2006.05.18	2006.05.31
	07-10～07-10-10		07-10-12	2006.03.01	2006.03.31
	07-00～07-00-/G		07-00-G3	2006.03.15	2006.03.31
P-9C12-2961	06-71～06-71-/L		06-71-/N	2006.02.16	2006.03.31
	06-51～06-51-/R		(注1)		2006.03.31
	06-00～06-00-/N		(注1)		2006.03.31
P-9S12-2971	07-50～07-50-05	Red Hat Linux(7.1/7.2/7.3)(x86版)Red Hat Enterprise Linux(AS 2.1/ES 2.1/WS 2.1)(x86版)Miracle Linux(x86版)	07-50-06	2005.11.25	2006.03.31
	07-11～07-11-06		07-11-08	2006.01.25	2006.03.31
	07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
P-9S12-	06-51～06-51-/R		06-51-/S	2006.05.09	2006.05.31

	2961	06-00～06-00-/N		(注1)		2006.03.31
	P-9S12-3971	07-50～07-50-05	Red Hat Enterprise Linux (AS 3/ES 3)(x86版)	07-50-06	2005.11.25	2006.03.31
		07-11～07-11-06		07-11-08	2006.01.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	P-9V12-2971	07-50～07-50-05	Red Hat Enterprise Linux(AS 3)(IPF版)	07-50-06	2005.11.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
	P-1612-296	06-51～06-51-B1	HI-UX/WE2	(注1)		2006.03.31
		06-00～06-00-G1		(注1)		2006.03.31
JP1/Automatic Job	P-2412-3N74	07-50～07-50-05	Windows (x86版)	07-50-06	2005.11.25	2006.03.31
		07-11～07-11-07		07-11-08	2006.01.25	2006.03.31
		07-10～07-10-11		07-10-12	2006.03.01	2006.03.31
		07-00～07-00-G2		07-00-G3	2006.03.15	2006.03.31
	P-2412-3N64	06-71～06-71-/M	Windows	06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-N1		(注1)		2006.03.31
	P-1B12-2A61	06-71～06-71-/M	HP-UX (PA-RISC版)	06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～				

Management System 2 - Light Edition		06-00-/N		(注1)		2006.03.31
	P-9112-2A61	06-71～06-71-/M	AIX	06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-/N		(注1)		2006.03.31
	P-9312-2A61	06-71～06-71-/M	Solaris	06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-/N		(注1)		2006.03.31
	P-9C12-2A61	06-71～06-71-/M	HP Tru64 UNIX	06-71-/N	2006.02.16	2006.03.31
		06-51～06-51-/R		(注1)		2006.03.31
		06-00～06-00-/N		(注1)		2006.03.31
	P-2412-3K77	07-50	Windows (x86版)	07-50-07	2006.03.08	2006.05.31
		07-00～07-00-G2		07-00-G3	2006.05.09	2006.05.31
	P-2812-3K77	07-50	Windows (IPF版)	07-50-07	2006.03.08	2006.05.31
	P-2412-3K67	06-71～06-71-/M	Windows	06-71-/N	2006.07.14	2006.09.29
		06-51～06-51-/N		(注1)		2006.05.31
		06-00～06-00-/A		(注1)		2006.05.31
	P-1B12-2772	07-50		07-50-07	2006.03.08	2006.05.31
		07-00～07-00-G2		07-00-G3	2006.05.09	2006.05.31

Job Management Partner 1/Automatic Job Management System 2 - Manager	P-1B12-2762	06-71～06-71-/M	HP-UX (PA-RISC版)	06-71-/N	2006.06.07	2006.09.29
		06-51～06-51-/N		(注1)		2006.05.31
	P-1J12-2772	07-50	HP-UX (IPF版)	07-50-07	2006.03.08	2006.05.31
	P-1M12-2772	07-50	AIX	07-50-07	2006.03.08	2006.05.31
		07-00～07-00-G2		07-00-G3	2006.05.09	2006.05.31
	P-9112-2762	06-71～06-71-/M		06-71-/N	2006.06.07	2006.09.29
		06-51～06-51-/N		(注1)		2006.05.31
	P-9312-2772	07-50	Solaris	07-50-07	2006.03.08	2006.05.31
		07-00～07-00-G2		07-00-G3	2006.05.09	2006.05.31
	P-9312-2762	06-71～06-71-/M		06-71-/N	2006.06.07	2006.09.29
		06-51～06-51-/N		(注1)		2006.05.31
	P-9C12-2762	06-71～06-71-/M	HP Tru64 UNIX	06-71-/N	2006.06.07	2006.09.29
		06-51～06-51-/N		(注1)		2006.05.31
	P-2412-3377	07-50	Windows (x86版)	07-50-07	2006.03.08	2006.05.31
		07-00～07-00-G2		07-00-G3	2006.05.09	2006.05.31
	P-2812-3377	07-50	Windows (IPF版)	07-50-07	2006.03.08	2006.05.31
		07-00		(注1)		2006.05.31
	P-2412-	06-71～06-71-J3	Windows	06-71-/N	2006.07.14	2006.09.29
		06-51～				

	3367	06-51-/N		(注1)		2006.05.31
		06-00		(注1)		2006.05.31
	P-1B12-2972	07-50	HP-UX (PA-RISC版)	07-50-07	2006.03.08	2006.05.31
		07-00～07-00-G2		07-00-G3	2006.05.09	2006.05.31
	P-1B12-2962	06-71～06-71-J3		06-71-/N	2006.05.22	2006.09.29
		06-51～06-51-/N		(注1)		2006.05.31
		06-00		(注1)		2006.05.31
Job Management Partner 1/Automatic Job Management System 2 - Agent	P-1J12-2972	07-50	HP-UX (IPF版)	07-50-07	2006.03.08	2006.05.31
		07-00		(注1)		2006.05.31
	P-1M12-2972	07-50	AIX	07-50-07	2006.03.08	2006.05.31
		07-00～07-00-G2		07-00-G3	2006.05.09	2006.05.31
	P-9112-2962	06-71～06-71-J3		06-71-/N	2006.05.22	2006.09.29
		06-51～06-51-/N		(注1)		2006.05.31
		06-00		(注1)		2006.05.31
	P-9312-2972	07-50	Solaris	07-50-07	2006.03.08	2006.05.31
		07-00～07-00-G2		07-00-G3	2006.05.09	2006.05.31
	P-9312-2962	06-71～06-71-J3		06-71-/N	2006.05.22	2006.09.29
		06-51～06-51-/N		(注1)		2006.05.31
		06-00		(注1)		2006.05.31
	P-9C12-2972	07-00～07-00-/G	HP Tru64 UNIX	07-00-G3	2006.05.09	2006.05.31
		06-71～06-71-J1		06-71-/N	2006.05.22	2006.09.29

	P-9C12-2962					
		06-51～06-51-/N		(注1)		2006.05.31
		06-00		(注1)		2006.05.31

(注1) 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。

- 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/AJS2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。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

JP1/AJS2で使用するポートの通信を信頼できるIPアドレスのみに限定するよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行なってください。

更新履歴 ：

- 2006.09.29 : [該当形名・バージョン，および対策版の提供]の形名P-

2412-3K67、P-1B12-2762、P-9112-2762、P-9312-2762、P-9C12-2762、P-2412-3367、P-1B12-2962、P-9112-2962、P-9312-2962、P-9C12-2962の対策バージョン、提供時期を更新しました。

- 2006.05.31 : [該当形名・バージョン，および対策版の提供]の形名P-2812-3374、P-1J12-2971、P-9C12-2971、P-9S12-2961の対策バージョン、提供時期を更新し、製品名、Job Management Partner 1/Automatic Job Management System 2 - ManagerとJob Management Partner 1/Automatic Job Management System 2 - Agentの情報を追記しました。
- 2006.03.31 : JP1製品におけるDoSの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

2008.02.04更新

HS06-007;

JP1製品におけるDoSの脆弱性

JP1/Performance Managementの対策

JP1/Performance Management(以下、JP1/PFMと略す)におきまして、意図しないデータを受信した場合、JP1/PFMのサービスが停止する場合があります。 JP1/PFMのサービスを再起動までは、JP1/Cm2/Network Node Manager連携機能、Agent Storeサービス、Master Storeサービスを使用した運用ができない可能性があります。

各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日
	P-242C-AV77	07-10		07-10-/B	2007.11.12	2008.02.04

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

JP1/Performance Management - Manager	P-242C-AA74	07-00～07-00-/O	Windows (x86)	07-00-/P	2005.05.17	2006.03.31
	P-242C-AA77	07-00		07-00-/A	2007.08.28	2008.02.04
	P-1B2C-AA71	07-00～07-00-/O	HP-UX (PA-RISC)	07-00-/P	2005.05.17	2006.03.31
	P-1B2C-AA72	07-00		07-00-/A	2007.08.28	2008.02.04
	P-1M2C-AA71	07-00～07-00-/O	AIX	07-00-/P	2005.05.17	2006.03.31
	P-1M2C-AA72	07-00		07-00-/A	2007.08.28	2008.02.04
	P-9D2C-AA71	07-00～07-00-/O	Solaris	07-00-/P	2005.05.17	2006.03.31
	P-9D2C-AA72	07-00		07-00-/A	2007.08.28	2008.02.04
	P-242C-AA64	06-70～06-70-/K	Windows (x86)	06-70-/M	2005.09.02	2006.03.31
	P-242C-AA67	06-70		(注1)		2008.02.04
	P-1B2C-AA61	06-70～06-70-/K	HP-UX (PA-RISC)	06-70-/M	2005.09.02	2006.03.31
	P-1B2C-AA62	06-70		(注2)		2008.02.04

	P-912C-AA61	06-70～06-70-/K	AIX	06-70-/M	2005.09.02	2006.03.31
	P-912C-AA62	06-70		(注3)		2008.02.04
	P-9D2C-AA61	06-70～06-70-/K	Solaris	06-70-/M	2005.09.02	2006.03.31
	P-9D2C-AA62	06-70		(注4)		2008.02.04
JP1/Performance Management - View	P-242C-AB74	07-00～07-00-/M	Windows (x86)	07-00-/N	2006.02.03	2006.03.31
	P-242C-AB77	07-00		07-00-/A	2007.09.06	2008.02.04
	P-1B2C-AB71	07-00～07-00-/M	HP-UX (PA-RISC)	07-00-/N	2006.02.03	2006.03.31
	P-9D2C-AB71	07-00～07-00-/M	Solaris	07-00-/N	2006.02.03	2006.03.31
	P-242C-AB64	06-70～06-70-/L	Windows (x86)	06-70-/M	2006.03.31	2006.03.31
	P-242C-AB67	06-70		(注5)		2008.02.04
	P-1B2C-AB61	06-70～06-70-/L	HP-UX (PA-RISC)	06-70-/M	2006.03.31	2006.03.31
	P-912C-AB61	06-70～06-70-/L	AIX	06-70-/M	2006.03.31	2006.03.31

	P-9D2C-AB61	06-70～06-70-/L	Solaris	06-70-/M	2006.03.31	2006.03.31
	P-242C-AC74	07-00～07-00-/O	Windows (x86)	07-00-/P	2005.05.26	2006.03.31
	P-242C-AC77	07-00		07-00-/B	2006.06.10	2006.09.29
	P-282C-AC74	07-00～07-00-/O	Windows (IPF)	07-00-/P	2005.05.26	2006.03.31
	P-1B2C-AC71	07-10～07-10-/B	HP-UX (PA-RISC)	07-10-/C	2005.06.02	2006.03.31
		07-00～07-00-/O		07-00-/P	2005.05.26	2006.03.31
	P-1B2C-AC72	07-00～07-00-/A		07-00-/B	2006.06.10	2006.09.29
	P-1J2C-AC71	07-10～07-10-/B	HP-UX (IPF)	07-10-/C	2005.06.02	2006.03.31
		07-00～07-00-/O		07-00-/P	2005.05.26	2006.03.31
	P-1M2C-AC71	07-10～07-10-/B	AIX	07-10-/C	2005.06.02	2006.03.31
		07-00～07-00-/O		07-00-/P	2005.05.26	2006.03.31
	P-1M2C-AC72	07-00～07-00-/A		07-00-/B	2006.06.10	2006.09.29
	P-9D2C-AC71	07-10～07-10-/B	Solaris	07-10-/C	2005.06.02	2006.03.31
		07-00～07-00-/O		07-00-/P	2005.05.26	2006.03.31
	P-					

JP1/Performance Management - Agent for Platform	9D2C-AC72	07-00～07-00-/A		07-00-/B	2006.06.10	2006.09.29
	P-9S2C-AC71	07-10～07-10-/B	Red Hat Enterprise Linux (AS 2.1)	07-10-/C	2005.06.02	2006.03.31
		07-00～07-00-/O		07-00-/P	2005.05.26	2006.03.31
	P-9S2C-BC71	07-10～07-10-/B	Red Hat Enterprise Linux (AS/ES 3.0)	07-10-/C	2005.06.02	2006.03.31
	P-242C-AC64	06-70～06-70-/L	Windows (x86)	06-70-/M	2005.10.27	2006.03.31
	P-242C-AC67	06-70		(注6)		2006.09.29
	P-1B2C-AC61	06-70～06-70-/L	HP-UX (PA-RISC)	06-70-/M	2005.10.27	2006.03.31
	P-1B2C-AC62	06-70		(注7)		2006.09.29
	P-912C-AC61	06-70～06-70-/L	AIX	06-70-/M	2005.10.27	2006.03.31
	P-912C-AC62	06-70		(注8)		2006.09.29
	P-9D2C-AC61	06-70～06-70-/L	Solaris	06-70-/M	2005.10.27	2006.03.31
	P-9D2C-AC62	06-70		(注9)		2006.09.29

	P-242C-AD74	07-10～07-10-/A	Windows (x86)	07-10-/C	2005.12.21	2006.03.31
		07-00～07-00-/Q		07-00-/R	2005.12.19	2006.03.31
	P-242C-AD77	07-00		07-00-/A	2006.08.08	2006.09.29
	P-282C-AD74	07-10～07-10-/A	Windows (IPF)	07-10-/C	2005.12.21	2006.03.31
		07-00～07-00-/N		07-00-/R	2005.12.19	2006.03.31
	P-1B2C-AD71	07-10～07-10-/A	HP-UX (PA-RISC)	07-10-/C	2005.12.21	2006.03.31
		07-00～07-00-/P		07-00-/R	2005.12.19	2006.03.31
	P-1B2C-AD72	07-00		07-00-/A	2006.08.08	2006.09.29
	P-1J2C-AD71	07-10～07-10-/A	HP-UX (IPF)	07-10-/C	2005.12.21	2006.03.31
		07-00～07-00-/P		07-00-/R	2005.12.19	2006.03.31
	P-1M2C-AD71	07-10～07-10-/A	AIX	07-10-/C	2005.12.21	2006.03.31
		07-00～07-00-/Q		07-00-/R	2005.12.19	2006.03.31
	P-1M2C-AD72	07-00		07-00-/A	2006.08.08	2006.09.29
JP1/Performance Management - Agent for Oracle	P-9D2C-AD71	07-10～07-10-/A	Solaris	07-10-/C	2005.12.21	2006.03.31
		07-00～07-00-/P		07-00-/R	2005.12.19	2006.03.31
	P-9D2C-	07-00		07-00-/A	2006.08.08	2006.09.29

	AD72					
	P-9S2C-AD71	07-10～07-10-/A	Red Hat Enterprise Linux (AS 2.1)	07-10-/C	2005.12.21	2006.03.31
		07-00～07-00-/Q		07-00-/R	2005.12.19	2006.03.31
	P-242C-AD64	06-70～06-70-/J	Windows (x86)	06-70-/K	2006.03.31	2006.03.31
	P-242C-AD67	06-70		(注10)		2006.09.29
	P-1B2C-AD61	06-70～06-70-/J	HP-UX (PA-RISC)	06-70-/K	2006.03.31	2006.03.31
	P-1B2C-AD62	06-70		(注11)		2006.09.29
	P-912C-AD61	06-70～06-70-/J	AIX	06-70-/K	2006.03.31	2006.03.31
	P-912C-AD62	06-70		(注12)		2006.09.29
	P-9D2C-AD61	06-70～06-70-/J	Solaris	06-70-/K	2006.03.31	2006.03.31
JP1/Performance Management - Agent for Microsoft SQL Server	P-242C-AE74	07-00～07-00-/K	Windows (x86)	07-00-/Q	2005.08.12	2006.03.31
	P-242C-AE77	07-00		07-00-/A	2006.08.10	2006.09.29
	P-282C-AE74	07-00～07-00-/O	Windows (IPF)	07-00-/Q	2005.08.12	2006.03.31

	P-242C-AE64	06-70～06-70-/J	Windows (x86)	06-70-/K	2006.03.31	2006.03.31
JP1/Performance Management - Agent for SAP R/3	P-242C-AF74	07-00～07-00-/L	Windows (x86)	07-00-/M	2005.11.02	2006.03.31
	P-242C-AF77	07-00		07-00-/O	2007.10.03	2008.02.04
	P-282C-AF74	07-00～07-00-/L	Windows (IPF)	07-00-/M	2005.11.02	2006.03.31
	P-1B2C-AF71	07-00～07-00-/L	HP-UX (PA-RISC)	07-00-/M	2005.11.02	2006.03.31
	P-1B2C-AF72	07-00		07-00-/O	2007.10.03	2008.02.04
	P-1J2C-AF71	07-00～07-00-/L	HP-UX (IPF)	07-00-/M	2005.11.02	2006.03.31
	P-1M2C-AF71	07-00～07-00-/L	AIX	07-00-/M	2005.11.02	2006.03.31
	P-1M2C-AF72	07-00		07-00-/O	2007.10.03	2008.02.04
	P-9D2C-AF71	07-00～07-00-/L	Solaris	07-00-/M	2005.11.02	2006.03.31
	P-9D2C-AF72	07-00		07-00-/O	2007.10.03	2008.02.04
	P-242C-AF64	06-70～06-70-/K	Windows (x86)	06-70-/M	2005.12.20	2006.03.31
	P-					

	1B2C-AF61	06-70～06-70-/K	HP-UX (PA-RISC)	06-70-/M	2005.12.20	2006.03.31
	P-912C-AF61	06-70～06-70-/K	AIX	06-70-/M	2005.12.20	2006.03.31
	P-9D2C-AF61	06-70～06-70-/K	Solaris	06-70-/M	2006.01.05	2006.03.31
JP1/Performance Management - Agent for HiRDB	P-242C-AK74	07-10～07-10-/C	Windows (x86)	07-10-/D	2005.08.12	2006.03.31
		07-00～07-00-/O		07-00-/Q	2005.08.25	2006.03.31
	P-282C-AK74	07-10～07-10-/C	Windows (IPF)	07-10-/D	2005.08.12	2006.03.31
		07-00～07-00-/O		07-00-/Q	2005.08.25	2006.03.31
	P-1B2C-AK71	07-10～07-10-/C	HP-UX (PA-RISC)	07-10-/D	2005.08.12	2006.03.31
		07-00～07-00-/O		07-00-/Q	2005.08.25	2006.03.31
	P-1J2C-AK71	07-10～07-10-/C	HP-UX (IPF)	07-10-/D	2005.08.12	2006.03.31
		07-00～07-00-/O		07-00-/Q	2005.08.25	2006.03.31
	P-1M2C-AK71	07-10～07-10-/C	AIX	07-10-/D	2005.08.12	2006.03.31
		07-00～07-00-/O		07-00-/Q	2005.08.25	2006.03.31
	P-9D2C-AK71	07-10～07-10-/C	Solaris	07-10-/D	2005.08.12	2006.03.31
		07-00～07-00-/O		07-00-/Q	2005.08.25	2006.03.31
	P-9S2C-	07-10～07-10-/C	Red Hat Enterprise	07-10-/D	2005.08.12	2006.03.31

	AK71	07-00～07-00-/O	Linux (AS 2.1)	07-00-/Q	2005.08.25	2006.03.31
	P-9S2C-BK71	07-10～07-10-/C	Red Hat Enterprise Linux (AS/ES 3.0)	07-10-/D	2005.08.12	2006.03.31
	P-242C-AK64	06-70～06-70-/L	Windows (x86)	06-70-/M	2005.09.29	2006.03.31
	P-1B2C-AK61	06-70～06-70-/L	HP-UX (PA-RISC)	06-70-/M	2005.09.29	2006.03.31
	P-912C-AK61	06-70～06-70-/L	AIX	06-70-/M	2005.09.29	2006.03.31
JP1/Performance Management - Agent for Domino	R-1529A-71	07-00～07-00-/K	Windows (x86)	07-00-/L	2005.09.08	2006.03.31
	R-1M29A-71	07-00～07-00-/K	AIX	07-00-/L	2005.09.08	2006.03.31
	R-1929A-71	07-00～07-00-/K	Solaris	07-00-/L	2005.09.08	2006.03.31
	R-1529A-61	06-70～06-70-/J	Windows (x86)	06-70-/K	2005.10.18	2006.03.31
	R-1929A-62	06-70～06-70-/J	AIX	06-70-/K	2005.10.18	2006.03.31
	R-1929A-61	06-70～06-70-/J	Solaris	06-70-/K	2005.10.18	2006.03.31
JP1/Performance Management -	R-	07-10～07-10-/A		07-10-/B	2006.04.06	2006.09.29

Agent for Microsoft Exchange Server	1529E-71	07-00～07-00-/O	Windows (x86)	07-00-/P	2006.04.06	2006.09.29
JP1/Performance Management - Agent for Microsoft Internet Information Server	R-1529F-71	07-10～07-10-/A	Windows (x86)	07-10-/B	2006.04.06	2006.09.29
		07-00～07-00-/O		07-00-/P	2006.04.06	2006.09.29
	R-1529H-71	07-10～07-10-/A	Windows (IPF)	07-10-/B	2006.04.06	2006.09.29

(注1) 本製品は、後継製品である形名P-242C-AA77の07-00-/A以降へのバージョンアップをお願いいたします。

(注2) 本製品は、後継製品である形名P-1B2C-AA72の07-00-/A以降へのバージョンアップをお願いいたします。

(注3) 本製品は、後継製品である形名P-1M2C-AA72の07-00-/A以降へのバージョンアップをお願いいたします。

(注4) 本製品は、後継製品である形名P-9D2C-AA72の07-00-/A以降へのバージョンアップをお願いいたします。

(注5) 本製品は、後継製品である形名P-242C-AB77の07-00-/A以降へのバージョンアップをお願いいたします。

(注6) 本製品は、後継製品である形名P-242C-AC77の07-00-/B以降へのバージョンアップをお願いいたします。

(注7) 本製品は、後継製品である形名P-1B2C-AC72の07-00-/B以降へのバージョンアップをお願いいたします。

(注8) 本製品は、後継製品である形名P-1M2C-AC72の07-00-/B以降へのバージョンアップをお願いいたします。

(注9) 本製品は、後継製品である形名P-9D2C-AC72の07-00-/B以降へのバージョンアップをお願いいたします。

(注10) 本製品は、後継製品である形名P-242C-AD77の07-00-/A以降への

バージョンアップをお願いいたします。

(注11) 本製品は、後継製品である形名P-1B2C-AD72の07-00-/A以降へのバージョンアップをお願いいたします。

(注12) 本製品は、後継製品である形名P-1M2C-AD72の07-00-/A以降へのバージョンアップをお願いいたします。

- 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/PFM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。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

JP1/PFM - Viewについては、NNM連携機能で使用するポート通信を信頼できるIPアドレスのみに限定するよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行なうことで回避可能です。
但し、JP1/PFM - ManagerやJP1/PFM - Agentのエクスポートまたはバックアップ機能については、回避策がございません。

更新履歴 ：

- 2008.02.04 : [該当形名・バージョン，および対策版の提供]の形名P-242C-AV77、P-242C-AA77、P-1B2C-AA72、P-1M2C-AA72、P-9D2C-AA72、P-242C-AA67、P-1B2C-AA62、P-912C-AA62、P-9D2C-AA62、P-242C-AB77、P-242C-AB67、P-242C-AF77、P-1B2C-AF72、P-1M2C-AF72、P-9D2C-AF72の対策バージョン、提供時期を更新しました。
- 2006.09.29 : [該当形名・バージョン，および対策版の提供]の形名P-242C-AC77、P-1B2C-AC72、P-1M2C-AC72、P-9D2C-AC72、P-242C-AC67、P-1B2C-AC62、P-912C-AC62、P-9D2C-AC62、P-242C-AD77、P-1B2C-AD72、P-1M2C-AD72、P-9D2C-AD72、P-242C-AD67、P-1B2C-AD62、P-912C-AD62、P-242C-AE77、R-1529E-71、R-1529F-71、R-1529H-71の対策バージョン、提供時期を更新しました。
- 2006.03.31 : JP1製品におけるDoSの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

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)

2006.03.31更新

HS06-007;

JP1製品におけるDoSの脆弱性

JP1/Cm2/Network Node Managerの対策

JP1/Cm2/Network Node Manager(以下、NNMと略す)におきまして，NNM のsnmpdmプロセスが使用しているポートに意図しないデータが送信された場合に、snmpdmプロセスがCPUを占有し、サービス不能に陥る可能性があります。

各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日
JP1/Cm2/Network Node Manager	P-2442-6274	07-00～07-01-/B	Windows	07-10-04 (注3)	2005.10.21	2006.03.31
	P-9D42-	07-00～	Solaris	07-10-04	2005.10.21	2006.03.31

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

	6271	07-01-/B		(注3)		
JP1/Cm2/Network Node Manager250	P-2442-6264	06-71-/D	Windows	06-71-SN	2006.03.31	2006.03.31
		06-00～06-71-/C		06-71-SN (注1)	2006.03.31	2006.03.31
	P-2442-6294	05-20～05-20-/F		(注4)		2006.03.31
	P-9D42-6261	06-71-/C	Solaris	06-71-SF (注2)	2006.03.31	2006.03.31
		06-00～06-71-/B		06-71-SF (注1)(注2)	2006.03.31	2006.03.31
	P-9D42-6211	05-20～05-20-/E		(注4)		2006.03.31
JP1/Cm2/Network Node ManagerEnterprise	P-2442-6164	06-71-/D	Windows	06-71-SN	2006.03.31	2006.03.31
		06-00～06-71-/C		06-71-SN (注1)	2006.03.31	2006.03.31
	P-2442-6194	05-20～05-20-/F		(注4)		2006.03.31
	P-9D42-6161	06-71-/C	Solaris	06-71-SF (注2)	2006.03.31	2006.03.31
		06-00～06-71-/B		06-71-SF (注1)(注2)	2006.03.31	2006.03.31
	P-9D42-6111	05-20～05-20-/E		(注4)		2006.03.31
Cm2/Network Node ManagerUnlimited	P-2442-5194	05-00～05-00-/A	Windows	(注4)		2006.03.31
Cm2/Network Node ManagerEnterprise	P-1642-511	05-00	HI-UX/WE2	(注4)		2006.03.31
	P-	05-00～				

Cm2/Network Node Manager250	2442-5294	05-00-/A	Windows	(注4)	2006.03.31
	P-1642-521	05-00	HI-UX/WE2	(注4)	2006.03.31

(注1) 本製品は、06-71最新修正版(Windows版の場合は06-71-/D、Solaris版の場合は06-71-/C)へのリビジョンアップ後、対策パッチの適用をお願いします。
なお、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。

(注2) Solaris版において、NNMとJP1/CM2/Extensible SNMP Agent(以下、ESA)と略すが同一サーバー内にインストールされていない場合にのみ、以下のNNMの対策パッチを適用してください(NNMとESAが同一サーバー内にインストールされている場合は、以下の対策パッチを適用する必要がありません)。
【Solaris版】

- P-9D42-6161対策パッチ: 06-71-SF
- P-9D42-6261 対策パッチ: 06-71-SF

(注3) 本製品は、リビジョンアップをお願いします(本問題については、07-10～07-10-03でも問題はありません)。
なお、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。

(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。

- 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

NNM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で使用するポートの通信を信頼できるIPアドレスのみに限定するよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行なってください。

更新履歴 ：

- 2006.03.31 : JP1製品におけるDoSの脆弱性の情報を公開しました。

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)

2006.03.31更新

HS06-007;

JP1製品におけるDoSの脆弱性

System Manager及びJP1/ServerConductorの対策

System Manager及びJP1/ServerConductorにおきまして、大量の不正な通信パケットを受信するとマネージャサービスが停止する場合があります。各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日
JP1/ServerConductor/Blade Server Manager	P-2418-6271	07-50, 07-50-/A, 07-51, 07-53, 07-55		07-63	2006.03.03	2006.03.31
	P-	07-50, 07-50-/A,				

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

	2418-3B6X	07-51, 07-53, 07-55		(注1)		2006.03.31
JP1/ServerConductor /Server Manager	P-2418-6371	07-50		07-50-/A	2006.03.14	2006.03.31
ServerConductor /Blade Server Manager	P-2418-6261	06-00, 06-00-/A		(注2)		2006.03.31
ServerConductor /Server Manager	P-2418-6361	06-00, 06-00-/A		(注3)		2006.03.31
System Manager - Management Console Version 5.0	P-2418-3154	05-00, 05-10, 05-20, 05-21, 05-30, 05-50-/A, 05-52-/A, 05-52-/B, 05-52-/C	Windows	05-52-/D	2006.03.31	2006.03.31
	P-2418-315U	05-00, 05-10, 05-20, 05-21, 05-30, 05-50-/A, 05-52-/A, 05-52-/B, 05-52-/C		05-52-/D	2006.03.31	2006.03.31
System Manager -	P-	03-00, 03-00-/A, 03-10, 03-20, 03-30, 03-30-/A, 03-31-/A,				

Management Console Version 3.0	2418-3134	03-40, 03-42, 03-44-/A, 03-50, 03-60, 03-60-/A, 03-60-/C, 03-60-/D		(注4)	2006.03.31

(注1) 本製品は、形名P-2418-6271のバージョン07-63以降へのリビジョンアップをお願いいたします。

(注2) 本製品は、後継製品である形名P-2418-6271の07-63以降へのバージョンアップをお願いいたします。

(注3) 本製品は、後継製品である形名P-2418-6371の07-50-/A以降へのバージョンアップをお願いいたします。

(注4) 本製品は、後継製品である形名P-2418-3154の05-52-/D以降へのバージョンアップをお願いいたします。

- 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
  System Manager及びJP1/ServerConductor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。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

System Manager及びJP1/ServerConductor/Blade Server Managerで使用するポートの通信を信頼できるIPアドレスのみに限定するよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行なってください。

更新履歴 ：

- 2006.03.31 : JP1製品におけるDoSの脆弱性の情報を公開しました。

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

2006.03.31更新

HS06-007;

JP1製品におけるDoSの脆弱性

JP1/File Access Controlの対策

JP1/File Access Control（以下，JP1/FACと略す）におきまして，意図しないデータを受信した場合に，JP1/FACサーバプロセス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、JP1/FACサーバプロセスを再起動させる必要があります。

各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日
JP1/File Access Control	P-1B2C-7A71	07-01	HP-UX	07-01-/A	2006.03.31	2006.03.31
	P-1B2C-7A61	06-72-A, 06-72-B		(注1)		2006.03.31
	P-242C-					

	7A74	07-00-/A	Windows	07-00-/B	2006.03.31	2006.03.31
	P-242C-7A64	06-72, 06-72-/B		(注2)		2006.03.31

(注1) 本製品の後継製品である形名P-1B2C-7A71の07-01-/A以降へのバージョンアップをお願いいたします。

(注2) 本製品の後継製品である形名P-242C-7A74の07-00-/B以降へのバージョンアップをお願いいたします。

- 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/FAC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。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

JP1/FACで使用するポートの通信を信頼できるIPアドレスのみに限定するよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行なってください。

更新履歴 ：

- 2006.03.31 : JP1製品におけるDoSの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

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

2006.03.31更新

HS06-007;

JP1製品におけるDoSの脆弱性

JP1/Security Integrated Managerの対策

JP1/Security Integrated Manager（以下，JP1/SCIMと略す）におきまして，意図しない接続が行なわれた場合、マネージャーからの通信が不可となり、ログ収集等ができなくなる場合があります。
各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日
JP1/Security Integrated Manager - Runtime Library	P-9D2C-7971	07-00, 07-01, 07-02, 07-10, 07-11, 07-11-/A	Solaris	07-11-/B	2006.03.31	2006.03.31

JP1/Security Integrated Manager	P-9D2C-7761	06-72, 06-73, 06-73-/A		06-73-/B	2006.03.31	2006.03.31

- 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/SCIM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。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

JP1/SCIMで使用するポートの通信を信頼できるIPアドレスのみに限定するよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行なってください。

更新履歴 ：

- 2006.03.31 : JP1製品におけるDoSの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

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)

2006.05.31更新

HS06-007;

JP1製品におけるDoSの脆弱性

JP1/ServerConductor/Deployment Managerの対策

JP1/ServerConductor/Deployment Managerにおきまして，大量の不正な通信パケットを受信すると以下のサービスが停止またはサービス不能に陥る場合があります。サービス不能となった場合は、JP1/ServerConductor/Deployment Managerのサービスを全て再起動させる必要があります。

- 管理サーバ for DPM
- クライアントサービス for DPM(Windows/Linux)

各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日

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

JP1/ServerConductor /Deployment Manager Standard Edition	R-1V15-12287A	07-50, 07-51, 07-52, 07-52-/A, 07-52-/B, 07-53, 07-54, 07-55	Windows（注２）	07-54-/A, 07-55-/A, 07-56	2006.5.31	2006.05.31
JP1/ServerConductor /Deployment Manager Enterprise Edition	R-1V15-12297A	07-52, 07-52-/A, 07-52-/B, 07-53, 07-54, 07-55		07-54-/A, 07-55-/A, 07-56	2006.5.31	2006.05.31
ServerConductor /DeploymentManager	R-1V15-11733A	01-00, 01-01, 06-00, 06-00-/A		（注１）		2006.05.31

(注1) 本製品は、後継製品である形名R-1V15-12287Aの07-54-/Aもしくは07-55-/A以降へのバージョンアップをお願いいたします。

(注2) クライアントサービス for DPMの適用OSはWindows/Linuxとなります。

- 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/ServerConductor/Deployment 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。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

JP1/ServerConductor/Deployment Managerで使用するポートの通信を信頼できるIPアドレスにのみに限定するよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行ってください。

更新履歴 ：

- 2006.05.31 : JP1製品におけるDoSの脆弱性の情報を公開しました。

- 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

2006.09.14更新

HS06-007;

JP1製品におけるDoSの脆弱性

JP1/Cm2/階層管理の対策

JP1/Cm2/階層管理におきまして、意図しないデータを受信した場合、階層管理機能がサービス不能に陥る可能性があります。

サービス不能になった場合は、OSを再起動させる必要があります。

各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日
	P-2442-6Y74	07-00～07-00-/B		07-10-10	2006.08.01	2006.09.14
		07-10～07-10-/A				2006.09.14
		06-00～06-00-/B				2006.09.14

JP1/Cm2/Hierarchical Agent	P-2442-6Y64	06-51～06-51-/A		06-71-/B	2006.09.11	2006.09.14
		06-71～06-71-/A				2006.09.14
	P-2442-6Y94	05-20		(注1)		2006.09.14
		05-21				2006.09.14
	P-2442-5Y94	05-00				2006.09.14
JP1/Cm2/SubManager	P-2442-6B74	07-00～07-00-/A	Windows (x86版)	07-10-/A	2006.08.09	2006.09.14
		07-10～07-10				2006.09.14
	P-2442-6B64	06-00～06-00-/B		06-71-/A	2006.09.11	2006.09.14
		06-51～06-51-/A				2006.09.14
		06-71				2006.09.14
	P-2442-6C64	06-00～06-00-/B		06-71-/A	2006.09.11	2006.09.14
		06-51～06-51-/A				2006.09.14
		06-71				2006.09.14
	P-2442-6D64	06-00～06-00-/B		06-71-/A	2006.09.11	2006.09.14
		06-51～06-51-/A				2006.09.14
		06-71				2006.09.14
	P-2442-5B94	05-00～05-00-/A		(注2)		2006.09.14
		05-20～05-20-/B				2006.09.14
		05-00～				2006.09.14

	P-2442-5C94	05-00-/A		(注3)	
		05-20～05-20-/B			2006.09.14
	P-2442-5D94	05-00～05-00-/A		(注4)	2006.09.14
		05-20～05-20-/B			2006.09.14

(注1) 本製品の後継製品である形名P-2442-6Y64の06-71-/B以降または、形名P-2442-6Y74の07-10-10以降へのバージョンアップをお願いいたします。

(注2) 本製品の後継製品である形名P-2442-6B64の06-71-/A以降または、形名P-2442-6B74の07-10-/A以降へのバージョンアップをお願いいたします。

(注3) 本製品の後継製品である形名P-2442-6C64の06-71-/A以降または、形名P-2442-6B74の07-10-/A以降へのバージョンアップをお願いいたします。

(注4) 本製品の後継製品である形名P-2442-6D64の06-71-/A以降または、形名P-2442-6B74の07-10-/A以降へのバージョンアップをお願いいたします。

- 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/階層管理に関しては，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。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

JP1/Cm2/階層管理で使用するポートの通信を信頼できるIPアドレスにのみに限定するよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行ってください。

更新履歴 ：

- 2006.09.14 : JP1製品におけるDoSの脆弱性の情報を公開しました。

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)

2007.07.06更新

HS06-007;

JP1製品におけるDoSの脆弱性

JP1/Baseの対策

JP1/Baseにおきまして、JP1/Baseが使用している通信ポートから、意図しないデータを受信した場合、JP1/Baseサービスが停止する場合があります。JP1/Baseサービスを再起動までは、JP1/Baseイベントサービス機能を使用したJP1イベントの運用ができない可能性があります。
各形名の最新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もしくはリビジョンアップをお願いします。

[該当形名・バージョン，および対策版の提供]

製品名	形名	対象バージョン	適用OS	対策バージョン	提供時期	更新日
	P-9D2C-	07-51～07-51-04		07-51-05	2006.05.15	2006.09.29
		07-50～07-50-07		07-50-08	2006.09.29	2006.11.08
		07-11～		07-11-09	2006.08.28	2006.09.29

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

JP1/Base	6L71	07-11-08	Solaris			
		07-10～07-10-C1		07-10-/F	2006.05.15	2006.09.29
		07-00～07-00-D1		07-00-/G	2006.07.28	2006.09.29
	P-9D2C-6L61	06-71～06-71-/M		(注１)		2006.09.29
		06-51～06-51-M2		(注１)		2006.09.29
Job Management Partner 1/Base	P-9D2C-6L72	07-51		07-51-09	2007.06.28	2007.07.06
	P-9D2C-6L62	06-51 ～06-51-/F		(注１)		2006.09.29
		06-71 ～06-71-/G		(注１)		2006.09.29

(注1) 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。

- 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/Base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。対策版へ入れ替えるまではこの暫定回避策を実施して下さい。

JP1/Baseで使用するポートの通信を信頼できるIPアドレスにのみに限定す

るよう、OSのIPフィルタリング機能またはルータ等にてフィルタリング設定を行ってください。

更新履歴 ：

- 2007.07.06 : [該当形名・バージョン，および対策版の提供]の形名P-9D2C-6L72の対策バージョン、提供時期を更新しました。
- 2006.11.08 : [該当形名・バージョン，および対策版の提供]の形名P-9D2C-6L71の対策バージョン、提供時期を更新しました。
- 2006.09.29 : JP1製品におけるDoSの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