TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: October 17, 2008

Vulnerability of DoS in JP1 Products

- Affected products

Corrective action	Product name	Platform	Last update
HS06-007-01	JP1/PFM/SNMP System Observer - Report Feature, JP1/Server System Observer - Report Feature	Windows	April 26, 2006
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	October 20, 2006
HS06-007-03	JP1/Performance Management - Manager, JP1/Performance Management - View, JP1/Performance Management - Agent	Windows, HP-UX, Solaris, AIX, Linux	February 4, 2008
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	April 26, 2006
HS06-007-05	JP1/Server Conductor/Blade Server Manager, JP1/Server Conductor/Server Manager, Server Conductor/Blade Server Manager, Server Conductor/Server Manager, System Manager - Management Console	Windows	April 26, 2006
HS06-007-06	JP1/File Access Control	Windows, HP-UX	April 26, 2006
HS06-007-07	JP1/Security Integrated Manager, JP1/Security Integrated Manager - Runtime Library	Solaris	April 26, 2006
	JP1/Server Conductor/Deployment Manager Standard Edition,		

HS06-007-08	JP1/Server Conductor/Deployment Manager Enterprise Edition, Server Conductor/Deployment Manager	Windows	June 20, 2006
HS06-007-09	The following JP1/Cm2 operation assist products: JP1/Cm2/Operations Assist Manager, JP1/Cm2/Operations Assist SubManager, JP1/Cm2/SubManager, JP1/Cm2/Operations Assist Agent, JP1/Cm2/Extensible Agent	Windows, HP-UX, Solaris, AIX, HI-UX/WE2	October 17, 2008
HS06-007-10	The following JP1/Cm2 hierarchical management products: JP1/Cm2/Hierarchical Agent, JP1/Cm2/SubManager	Windows	October 20, 2006
HS06-007-11	JP1/Base, Job Management Partner 1/Base	Solaris	July 6, 2007

- Problem description

When the above products receive requests or data unexpectedly, the processing of such products sometimes stop, or a reply fails to be sent.
Malicious remote users can exploit this vulnerability and cause DoS in the above products.

Revision history

- October 17, 2008: Corrective actions page of HS06-007-09 is updated.
- February 4, 2008: Corrective actions page of HS06-007-03 is updated.
- July 6, 2007: Corrective actions page of HS06-007-11 is updated.
- February 15, 2007: Corrective actions page of HS06-007-09 is updated.
- November 8, 2006: Corrective actions page of HS06-007-11 is newly added.
- October 20, 2006: Corrective actions pages of HS06-007-09 and HS06-007-10 are newly added.
  Corrective actions pages of HS06-007-02 and HS06-007-03 are updated.
- June 20, 2006: Corrective actions page of HS06-007-08 is newly added.
- May 31, 2006: Corrective actions page of HS06-007-02 is updated.
  Job Management Partner 1/Automatic Job Management System 2 - Manager and Job Management Partner 1/Automatic Job Management System 2 - Agent are added to the Affected products.
- April 26, 2006: This page is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.

- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

©Hitachi, Ltd. 1994, 2008. All rights reserved.

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: April 26, 2006

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for JP1/PFM/SNMP System Observer - Report Feature

If JP1/PFM/SNMP System Observer - Report Feature receives data unexpectedly, a DoS (Denial of Service) might occur. In this case, restart the server process of JP1/PFM/SNMP System Observer - Report Feature or restart the OS.
Fixed versions for the recent versions are available indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
JP1/Server System Observer - Report Feature	P-F2442-6R641	06-71 to 06-71-/D	Windows	06-71-/E	March 31, 2006	April 26, 2006
JP1/Server System Observer - Report Feature	P-F2442-6R671	06-71		(*1)		April 26, 2006
JP1/PFM/SNMP System Observer - Report Feature	P-F242C-6T741	07-00 to 07-00-/A		07-00-/B	February 16, 2006	April 26, 2006
		07-10 to 07-10-/A		07-10-/B	March 31, 2006	April 26, 2006
		07-50		07-50-01	February 6, 2006	April 26, 2006
JP1/PFM/SNMP System Observer - Report Feature	P-F242C-6T771	07-00		(*1)		April 26, 2006

(*1) For detailed information about this model, contact your Hitachi support service representative.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, carry out the following workarounds:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the port that JP1/PFM/SNMP System Observer - Report Feature uses.

Revision history

- April 26, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

| Term of Use | Privacy Notice | About Hitachi |

©Hitachi, Ltd. 1994, 2008. All rights reserved.

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: October 20, 2006

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for JP1/Automatic Job Management System 2

If JP1/Automatic Job Management System 2 (JP1/AJS2) receives data unexpectedly through the port, the JP1/AJS2 service might stop. Until the JP1/AJS2 service is rebooted, batch job operations that use JP1/AJS2 might be disabled.
Fixed versions for the recent versions are available indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
	P-2412-3K74	07-50 to 07-50-05	Windows (x86)	07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-07		07-11-08	January 25, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
		07-00 to 07-00-G2		07-00-G3	March 15, 2006	April 26, 2006
	P-2812-3K74	07-50 to 07-50-05	Windows (IPF)	07-50-06	November 25, 2005	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	P-2412-3K64	06-71 to 06-71-/M	Windows	06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-N1		(*1)		April 26,

						2006
JP1/Automatic Job Management System 2 - Manager	P-1B12-2771	07-50 to 07-50-05	HP-UX (PA-RISC)	07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-07		07-11-08	January 25, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
		07-00 to 07-00-G2		07-00-G3	March 15, 2006	April 26, 2006
	P-1B12-2761	06-71 to 06-71-/M		06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-/N		(*1)		April 26, 2006
	P-1J12-2771	07-50 to 07-50-05	HP-UX (IPF)	07-50-06	November 25, 2005	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	P-1M12-2771	07-50 to 07-50-05	AIX	07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-07		07-11-08	January 25, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
		07-00 to 07-00-G2		07-00-G3	March 15, 2006	April 26, 2006
	P-9112-2761	06-71 to 06-71-/M		06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-/N		(*1)		April 26, 2006
	P-9312-2771	07-50 to 07-50-05		07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-07		07-11-08	February 13, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006

		07-00 to 07-00-G2	Solaris	07-00-G3	March 15, 2006	April 26, 2006
	P-9312-2761	06-71 to 06-71-/M		06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-/N		(*1)		April 26, 2006
	P-9C12-2761	06-71 to 06-71-/M	HP Tru64 UNIX	06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-N		(*1)		April 26, 2006
	P-9S12-2771	07-50 to 07-50-05	Red Hat Linux (7.1/7.2/7.3)(x86), Red Hat Enterprise Linux (AS 2.1/ES 2.1/WS 2.1)(x86), Miracle Linux (x86)	07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-07		07-11-08	January 25, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	P-9S12-3771	07-50 to 07-50-05	Red Hat Enterprise Linux (AS 3/ES 3)(x86)	07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-07		07-11-08	January 25, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	P-9V12-2771	07-50 to 07-50-05	Red Hat Enterprise Linux (AS 3)(IPF)	07-50-06	November 25, 2005	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	P-2412-3374	07-50 to 07-50-05	Windows (x86)	07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-06		07-11-08	January 25, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
		07-00 to 07-00-G2		07-00-G3	March 15, 2006	April 26, 2006
						April

P-2812-3374	07-50 to 07-50-05	Windows (IPF)	07-50-06	November 25, 2005	April 26, 2006
	07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	07-00		07-00-G3	March 15, 2006	April 26, 2006
			07-00-/G	April 6, 2006	May 31, 2006
P-2412-3364	06-71 to 06-71-/L	Windows	06-71-/N	February 16, 2006	April 26, 2006
	06-51 to 06-51-/R		(*1)		April 26, 2006
	06-00 to 06-00-N		(*1)		April 26, 2006
P-1B12-2971	07-50 to 07-50-05	HP-UX (PA-RISC)	07-50-06	November 25, 2005	April 26, 2006
	07-11 to 07-11-06		07-11-08	January 25, 2006	April 26, 2006
	07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	07-00 to 07-00-G2		07-00-G3	March 15, 2006	April 26, 2006
P-1B12-2961	06-71 to 06-71-/L		06-71-/N	February 16, 2006	April 26, 2006
	06-51 to 06-51-/R		(*1)		April 26, 2006
	06-00 to 06-00-/N		(*1)		April 26, 2006
P-1J12-2971	07-50 to 07-50-05	HP-UX (IPF)	07-50-06	November 25, 2005	April 26, 2006
	07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	07-00		07-00-G3	March 15, 2006	April 26, 2006
			07-00-/G	March 29, 2006	May 31, 2006
	07-50 to 07-50-05		07-50-06	November 25, 2005	April 26, 2006
	07-11 to			January	April

JP1/Automatic Job Management System 2 - Agent	P-1M12-2971	07-11-06	AIX	07-11-08	25, 2006	26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
		07-00 to 07-00-G2		07-00-G3	March 15, 2006	April 26, 2006
	P-9112-2961	06-71 to 06-71-/L		06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-/N		(*1)		April 26, 2006
	P-9312-2971	07-50 to 07-50-05	Solaris	07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-06		07-11-08	February 13, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
		07-00 to 07-00-G2		07-00-G3	March 15, 2006	April 26, 2006
	P-9312-2961	06-71 to 06-71-/L		06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-/N		(*1)		April 26, 2006
	P-9C12-2971	07-11	HP Tru64 UNIX	07-10-09	May 18, 2006	May 31, 2006
		07-10 to 07-10-10		07-10-12	March 1, 2006	April 26, 2006
		07-00 to 07-00-/G		07-00-G3	March 15, 2006	April 26, 2006
	P-9C12-2961	06-71 to 06-71-/L		06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-N		(*1)		April 26, 2006
		07-50 to		07-50-06	November	April 26,

	P-9S12-2971	07-50-05	Red Hat Linux (7.1/7.2/7.3)(x86), Red Hat Enterprise Linux (AS 2.1/ES 2.1/WS 2.1)(x86), Miracle Linux (x86)		25, 2005	2006
		07-11 to 07-11-06		07-11-08	January 25, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
		07-00 to 07-00-G2		07-00-G3	March 15, 2006	April 26, 2006
	P-9S12-2961	06-51 to 06-51-/R		06-51-/S	May 9, 2006	May 31, 2006
		06-00 to 06-00-/N		(*1)		April 26, 2006
	P-9S12-3971	07-50 to 07-50-05	Red Hat Enterprise Linux (AS 3/ES 3)(x86)	07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-06		07-11-08	January 25, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	P-9V12-2971	07-50 to 07-50-05	Red Hat Enterprise Linux (AS 3)(IPF)	07-50-06	November 25, 2005	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
	P-1612-296	06-51 to 06-51-B1	HI-UX/WE2	(*1)		April 26, 2006
		06-00 to 06-00-G1		(*1)		April 26, 2006
	P-2412-3N74	07-50 to 07-50-05	Windows (x86)	07-50-06	November 25, 2005	April 26, 2006
		07-11 to 07-11-07		07-11-08	January 25, 2006	April 26, 2006
		07-10 to 07-10-11		07-10-12	March 1, 2006	April 26, 2006
		07-00 to 07-00-G2		07-00-G3	March 15, 2006	April 26, 2006
	P-2412-3N64	06-71 to 06-71-/M	Windows	06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-N1		(*1)		April 26,

JP1/Automatic Job Management System 2 - Light Edition						2006
	P-1B12-2A61	06-71 to 06-71-/M	HP-UX (PA-RISC)	06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-/N		(*1)		April 26, 2006
	P-9112-2A61	06-71 to 06-71-/M	AIX	06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-/N		(*1)		April 26, 2006
	P-9312-2A61	06-71 to 06-71-/M	Solaris	06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-/N		(*1)		April 26, 2006
	P-9C12-2A61	06-71 to 06-71-/M	HP Tru64 UNIX	06-71-/N	February 16, 2006	April 26, 2006
		06-51 to 06-51-/R		(*1)		April 26, 2006
		06-00 to 06-00-N		(*1)		April 26, 2006
	P-2412-3K77	07-50	Windows (x86)	07-50-07	March 8, 2006	May 31, 2006
		07-00 to 07-00-G2		07-00-G3	May 9, 2006	May 31, 2006
	P-2812-3K77	07-50	Windows (IPF)	07-50-07	March 8, 2006	May 31, 2006
	P-2412-3K67	06-71 to 06-71-/M	Windows	06-71-/N	July 14, 2006	October 20, 2006
		06-51 to 06-51-/N		(*1)		May 31, 2006
		06-00 to 06-00-/A		(*1)		May 31, 2006
		07-50		07-50-07	March 8, 2006	May 31, 2006

Job Management Partner 1/Automatic Job Management System 2 - Manager	P-1B12-2772	07-00 to 07-00-G2	HP-UX (PA-RISC)	07-00-G3	May 9, 2006	May 31, 2006
	P-1B12-2762	06-71 to 06-71-/M		06-71-/N	June 7, 2006	October 20, 2006
		06-51 to 06-51-/N		(*1)		May 31, 2006
	P-1J12-2772	07-50	HP-UX (IPF)	07-50-07	March 8, 2006	May 31, 2006
	P-1M12-2772	07-50	AIX	07-50-07	March 8, 2006	May 31, 2006
		07-00 to 07-00-G2		07-00-G3	May 9, 2006	May 31, 2006
	P-9112-2762	06-71 to 06-71-/M		06-71-/N	June 7, 2006	October 20, 2006
		06-51 to 06-51-/N		(*1)		May 31, 2006
	P-9312-2772	07-50	Solaris	07-50-07	March 8, 2006	May 31, 2006
		07-00 to 07-00-G2		07-00-G3	May 9, 2006	May 31, 2006
	P-9312-2762	06-71 to 06-71-/M		06-71-/N	June 7, 2006	October 20, 2006
		06-51 to 06-51-/N		(*1)		May 31, 2006
	P-9C12-2762	06-71 to 06-71-/M	HP Tru64 UNIX	06-71-/N	June 7, 2006	October 20, 2006
		06-51 to 06-51-/N		(*1)		May 31, 2006
	P-2412-3377	07-50	Windows (x86)	07-50-07	March 8, 2006	May 31, 2006
		07-00 to 07-00-G2		07-00-G3	May 9, 2006	May 31, 2006
	P-2812-3377	07-50	Windows (IPF)	07-50-07	March 8, 2006	May 31, 2006
		07-00		(*1)		May 31, 2006
		06-71 to 06-71-J3		06-71-/N	July 14, 2006	October 20, 2006

Job Management Partner 1/Automatic Job Management System 2 - Agent	P-2412-3367	06-51 to 06-51-/N	Windows	(*1)		May 31, 2006
		06-00		(*1)		May 31, 2006
	P-1B12-2972	07-50	HP-UX (PA-RISC)	07-50-07	March 8, 2006	May 31, 2006
		07-00 to 07-00-G2		07-00-G3	May 9, 2006	May 31, 2006
	P-1B12-2962	06-71 to 06-71-J3		06-71-/N	May 22, 2006	October 20, 2006
		06-51 to 06-51-/N		(*1)		May 31, 2006
		06-00		(*1)		May 31, 2006
	P-1J12-2972	07-50	HP-UX (IPF)	07-50-07	March 8, 2006	May 31, 2006
		07-00		(*1)		May 31, 2006
	P-1M12-2972	07-50	AIX	07-50-07	March 8, 2006	May 31, 2006
		07-00 to 07-00-G2		07-00-G3	May 9, 2006	May 31, 2006
	P-9112-2962	06-71 to 06-71-J3		06-71-/N	May 22, 2006	October 20, 2006
		06-51 to 06-51-/N		(*1)		May 31, 2006
		06-00		(*1)		May 31, 2006
	P-9312-2972	07-50	Solaris	07-50-07	March 8, 2006	May 31, 2006
		07-00 to 07-00-G2		07-00-G3	May 9, 2006	May 31, 2006
	P-9312-2962	06-71 to 06-71-J3		06-71-/N	May 22, 2006	October 20, 2006
		06-51 to 06-51-/N		(*1)		May 31, 2006
		06-00		(*1)		May 31, 2006
						May

	P-9C12-2972	07-00 to 07-00-/G	HP Tru64 UNIX	07-00-G3	May 9, 2006	31, 2006
	P-9C12-2962	06-71 to 06-71-J1		06-71-/N	May 22, 2006	October 20, 2006
		06-51 to 06-51-/N		(*1)		May 31, 2006
		06-00		(*1)		May 31, 2006

(*1) For detailed information about this model, contact your Hitachi support service representative.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, carry out the following workarounds:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the port that JP1/AJS2 uses.

Revision history

- October 20, 2006: Information about fixed versions and release time of 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 is updated.
- May 31, 2006: Information about fixed versions and release time of P-2812-3374, P-1J12-2971, P-9C12-2971 and P-9S12-2961 is updated.
  Information of Job Management Partner 1/Automatic Job Management System 2 - Manager and Job Management Partner 1/Automatic Job Management System 2 - Agent products is added.
- April 26, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in

connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.

- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

©Hitachi, Ltd. 1994, 2008. All rights reserved.

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: February 4, 2008

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for JP1/Performance Management

If JP1/Performance Management (JP1/PFM) receives data unexpectedly, the JP1/PFM service might stop. Until the JP1/AJS2 service is rebooted, operations that use JP1/Cm2/Network Node Manager, the Agent Store service, and the Master Store service might be disabled.
Fixed versions for the recent versions are available indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
JP1/Performance Management - Manager	P-242C-AV77	07-10	Windows (x86)	07-10-/B	November 12, 2007	February 4, 2008
	P-242C-AA74	07-00 to 07-00-/O		07-00-/P	May 17, 2005	April 26, 2006
	P-242C-AA77	07-00		07-00-/A	August 28, 2007	February 4, 2008
	P-242C-AA64	06-70 to 06-70-/K		06-70-/M	September 2, 2005	April 26, 2006
	P-242C-AA67	06-70		(*1)		February 4, 2008
	P-1B2C-AA71	07-00 to 07-00-/O	HP-UX (PA-RISC)	07-00-/P	May 17, 2005	April 26, 2006
	P-1B2C-AA72	07-00		07-00-/A	August 28, 2007	February 4, 2008
	P-1B2C-AA61	06-70 to 06-70-/K		06-70-/M	September 2, 2005	April 26, 2006
	P-1B2C-AA62	06-70		(*2)		February 4, 2008
	P-1M2C-AA71	07-00 to 07-00-/O	AIX	07-00-/P	May 17, 2005	April 26, 2006
	P-1M2C-AA72	07-00		07-00-/A	August 28, 2007	February 4, 2008
	P-912C-AA61	06-70 to 06-70-/K		06-70-/M	September 2, 2005	April 26, 2006
						February

	P-912C-AA62	06-70		(*3)		4, 2008
	P-9D2C-AA71	07-00 to 07-00-/O	Solaris	07-00-/P	May 17, 2005	April 26, 2006
	P-9D2C-AA72	07-00		07-00-/A	August 28, 2007	February 4, 2008
	P-9D2C-AA61	06-70 to 06-70-/K		06-70-/M	September 2, 2005	April 26, 2006
	P-9D2C-AA62	06-70		(*4)		February 4, 2008
JP1/Performance Management - View	P-242C-AB74	07-00 to 07-00-/M	Windows (x86)	07-00-/N	February 3, 2006	April 26, 2006
	P-242C-AB77	07-00		07-00-/A	September 6, 2007	February 4, 2008
	P-242C-AB64	06-70 to 06-70-/L		06-70-/M	March 31, 2006	April 26, 2006
	P-242C-AB67	06-70		(*5)		February 4, 2008
	P-1B2C-AB71	07-00 to 07-00-/M	HP-UX (PA-RISC)	07-00-/N	February 3, 2006	April 26, 2006
	P-1B2C-AB61	06-70 to 06-70-/L		06-70-/M	March 31, 2006	April 26, 2006
	P-912C-AB61	06-70 to 06-70-/L	AIX	06-70-/M	March 31, 2006	April 26, 2006
	P-9D2C-AB71	07-00 to 07-00-/M	Solaris	07-00-/N	February 3, 2006	April 26, 2006
	P-9D2C-AB61	06-70 to 06-70-/L		06-70-/M	March 31, 2006	April 26, 2006
JP1/Performance Management - Agent for Platform	P-242C-AC74	07-00 to 07-00-/O	Windows (x86)	07-00-/P	May 26, 2005	April 26, 2006
	P-242C-AC77	07-00		07-00-/B	June 10, 2006	October 20, 2006
	P-242C-AC64	06-70 to 06-70-/L		06-70-/M	October 27, 2005	April 26, 2006
	P-242C-AC67	06-70		(*6)		October 20, 2006
	P-282C-AC74	07-00 to 07-00-/O	Windows (IPF)	07-00-/P	May 26, 2005	April 26, 2006
	P-1B2C-AC71	07-10 to 07-10-/B	HP-UX (PA-RISC)	07-10-/C	June 2, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/P	May 26, 2005	April 26, 2006
	P-1B2C-AC72	07-00 to 07-00-/A		07-00-/B	June 10, 2006	October 20, 2006
	P-1B2C-AC61	06-70 to 06-70-/L		06-70-/M	October 27, 2005	April 26, 2006
	P-1B2C-AC62	06-70		(*7)		October 20, 2006
	P-1J2C-AC71	07-10 to 07-10-/B	HP-UX (IPF)	07-10-/C	June 2, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/P	May 26, 2005	April 26, 2006
	P-1M2C-AC71	07-10 to 07-10-/B		07-10-/C	June 2, 2005	April 26, 2006
		07-00 to		07-00-/P	May 26,	April

		07-00-/O			2005	26, 2006
	P-1M2C-AC72	07-00 to 07-00-/A	AIX	07-00-/B	June 10, 2006	October 20, 2006
	P-912C-AC61	06-70 to 06-70-/L		06-70-/M	October 27, 2005	April 26, 2006
	P-912C-AC62	06-70		(*8)		October 20, 2006
	P-9D2C-AC71	07-10 to 07-10-/B	Solaris	07-10-/C	June 2, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/P	May 26, 2005	April 26, 2006
	P-9D2C-AC72	07-00 to 07-00-/A		07-00-/B	June 10, 2006	October 20, 2006
	P-9D2C-AC61	06-70 to 06-70-/L		06-70-/M	October 27, 2005	April 26, 2006
	P-9D2C-AC62	06-70		(*9)		October 20, 2006
	P-9S2C-AC71	07-10 to 07-10-/B	Red Hat Enterprise Linux (AS 2.1)	07-10-/C	June 2, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/P	May 26, 2005	April 26, 2006
	P-9S2C-BC71	07-10 to 07-10-/B	Red Hat Enterprise Linux (AS/ES 3.0)	07-10-/C	June 2, 2005	April 26, 2006
JP1/Performance Management - Agent for Oracle	P-242C-AD74	07-10 to 07-10-/A	Windows (x86)	07-10-/C	December 21, 2005	April 26, 2006
		07-00 to 07-00-/Q		07-00-/R	December 19, 2005	April 26, 2006
	P-242C-AD77	07-00		07-00-/A	August 8, 2006	October 20, 2006
	P-242C-AD64	06-70 to 06-70-/J		06-70-/K	March 31, 2006	April 26, 2006
	P-242C-AD67	06-70		(*10)		October 20, 2006
	P-282C-AD74	07-10 to 07-10-/A	Windows (IPF)	07-10-/C	December 21, 2005	April 26, 2006
		07-00 to 07-00-/N		07-00-/R	December 19, 2005	April 26, 2006
	P-1B2C-AD71	07-10 to 07-10-/A	HP-UX (PA-RISC)	07-10-/C	December 21, 2005	April 26, 2006
		07-00 to 07-00-/P		07-00-/R	December 19, 2005	April 26, 2006
	P-1B2C-AD72	07-00		07-00-/A	August 8, 2006	October 20, 2006
	P-1B2C-AD61	06-70 to 06-70-/J		06-70-/K	March 31, 2006	April 26, 2006
	P-1B2C-AD62	06-70		(*11)		October 20, 2006
	P-1J2C-AD71	07-10 to 07-10-/A	HP-UX (IPF)	07-10-/C	December 21, 2005	April 26, 2006
		07-00 to 07-00-/P		07-00-/R	December 19, 2005	April 26, 2006
		07-10 to		07-10-/C	December	April

	P-1M2C-AD71	07-10-/A	AIX		21, 2005	26, 2006
		07-00 to 07-00-/Q		07-00-/R	December 19, 2005	April 26, 2006
	P-1M2C-AD72	07-00		07-00-/A	August 8, 2006	October 20, 2006
	P-912C-AD61	06-70 to 06-70-/J		06-70-/K	March 31, 2006	April 26, 2006
	P-912C-AD62	06-70		(*12)		October 20, 2006
	P-9D2C-AD71	07-10 to 07-10-/A	Solaris	07-10-/C	December 21, 2005	April 26, 2006
		07-00 to 07-00-/P		07-00-/R	December 19, 2005	April 26, 2006
	P-9D2C-AD72	07-00		07-00-/A	August 8, 2006	October 20, 2006
	P-9D2C-AD61	06-70 to 06-70-/J		06-70-/K	March 31, 2006	April 26, 2006
	P-9S2C-AD71	07-10 to 07-10-/A	Red Hat Enterprise Linux (AS 2.1)	07-10-/C	December 21, 2005	April 26, 2006
		07-00 to 07-00-/Q		07-00-/R	December 19, 2005	April 26, 2006
JP1/Performance Management - Agent for Microsoft SQL Server	P-242C-AE74	07-00 to 07-00-/K	Windows (x86)	07-00-/Q	August 12, 2005	April 26, 2006
	P-242C-AE77	07-00		07-00-/A	August 10, 2006	October 20, 2006
	P-242C-AE64	06-70 to 06-70-/J		06-70-/K	March 31, 2006	April 26, 2006
	P-282C-AE74	07-00 to 07-00-/O	Windows (IPF)	07-00-/Q	August 12, 2005	April 26, 2006
JP1/Performance Management - Agent for SAP R/3	P-242C-AF74	07-00 to 07-00-/L	Windows (x86)	07-00-/M	November 2, 2005	April 26, 2006
	P-242C-AF77	07-00		07-00-/O	October 3, 2007	February 4, 2008
	P-242C-AF64	06-70 to 06-70-/K		06-70-/M	December 20, 2005	April 26, 2006
	P-282C-AF74	07-00 to 07-00-/L	Windows (IPF)	07-00-/M	November 2, 2005	April 26, 2006
	P-1B2C-AF71	07-00 to 07-00-/L	HP-UX (PA-RISC)	07-00-/M	November 2, 2005	April 26, 2006
	P-1B2C-AF72	07-00		07-00-/O	October 3, 2007	February 4, 2008
	P-1B2C-AF61	06-70 to 06-70-/K		06-70-/M	December 20, 2005	April 26, 2006
	P-1J2C-AF71	07-00 to 07-00-/L	HP-UX (IPF)	07-00-/M	November 2, 2005	April 26, 2006
	P-1M2C-AF71	07-00 to 07-00-/L	AIX	07-00-/M	November 2, 2005	April 26, 2006
	P-1M2C-AF72	07-00		07-00-/O	October 3, 2007	February 4, 2008
	P-912C-AF61	06-70 to 06-70-/K		06-70-/M	December 20, 2005	April 26, 2006
	P-9D2C-AF71	07-00 to 07-00-/L	Solaris	07-00-/M	November 2, 2005	April 26, 2006
	P-9D2C-AF72	07-00		07-00-/O	October 3, 2007	February 4, 2008

	P-9D2C-AF61	06-70 to 06-70-/K		06-70-/M	January 5, 2006	April 26, 2006
JP1/Performance Management - Agent for HiRDB	P-242C-AK74	07-10 to 07-10-/C	Windows (x86)	07-10-/D	August 12, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/Q	August 25, 2005	April 26, 2006
	P-242C-AK64	06-70 to 06-70-/L		06-70-/M	September 29, 2005	April 26, 2006
	P-282C-AK74	07-10 to 07-10-/C	Windows (IPF)	07-10-/D	August 12, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/Q	August 25, 2005	April 26, 2006
	P-1B2C-AK71	07-10 to 07-10-/C	HP-UX (PA-RISC)	07-10-/D	August 12, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/Q	August 25, 2005	April 26, 2006
	P-1B2C-AK61	06-70 to 06-70-/L		06-70-/M	September 29, 2005	April 26, 2006
	P-1J2C-AK71	07-10 to 07-10-/C	HP-UX (IPF)	07-10-/D	August 12, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/Q	August 25, 2005	April 26, 2006
	P-1M2C-AK71	07-10 to 07-10-/C	AIX	07-10-/D	August 12, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/Q	August 25, 2005	April 26, 2006
	P-912C-AK61	06-70 to 06-70-/L		06-70-/M	September 29, 2005	April 26, 2006
	P-9D2C-AK71	07-10 to 07-10-/C	Solaris	07-10-/D	August 12, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/Q	August 25, 2005	April 26, 2006
	P-9S2C-AK71	07-10 to 07-10-/C	Red Hat Enterprise Linux (AS 2.1)	07-10-/D	August 12, 2005	April 26, 2006
		07-00 to 07-00-/O		07-00-/Q	August 25, 2005	April 26, 2006
	P-9S2C-BK71	07-10 to 07-10-/C	Red Hat Enterprise Linux (AS/ES 3.0)	07-10-/D	August 12, 2005	April 26, 2006
JP1/Performance Management - Agent for Domino	R-1529A-71	07-00 to 07-00-/K	Windows (x86)	07-00-/L	September 8, 2005	April 26, 2006
	R-1529A-61	06-70 to 06-70-/J		06-70-/K	October 18, 2005	April 26, 2006
	R-1M29A-71	07-00 to 07-00-/K	AIX	07-00-/L	September 8, 2005	April 26, 2006
	R-1929A-62	06-70 to 06-70-/J		06-70-/K	October 18, 2005	April 26, 2006
	R-1929A-71	07-00 to 07-00-/K	Solaris	07-00-/L	September 8, 2005	April 26, 2006
	R-1929A-61	06-70 to 06-70-/J		06-70-/K	October 18, 2005	April 26, 2006
JP1/Performance Management - Agent for Microsoft	R-1529E-71	07-10 to 07-10-/A	Windows (x86)	07-10-/B	April 6, 2006	October 20, 2006

Exchange Server		07-00 to 07-00-/O		07-00-/P	April 6, 2006	October 20, 2006
JP1/Performance Management - Agent for Microsoft Internet Information Server	R-1529F-71	07-10 to 07-10-/A	Windows (x86)	07-10-/B	April 6, 2006	October 20, 2006
		07-00 to 07-00-/O		07-00-/P	April 6, 2006	October 20, 2006
	R-1529H-71	07-10 to 07-10-/A	Windows (IPF)	07-10-/B	April 6, 2006	October 20, 2006

(*1) Please upgrade the version to 07-00-/A of the succeeding model P-242C-AA77 or later.
(*2) Please upgrade the version to 07-00-/A of the succeeding model P-1B2C-AA72 or later.
(*3) Please upgrade the version to 07-00-/A of the succeeding model P-1M2C-AA72 or later.
(*4) Please upgrade the version to 07-00-/A of the succeeding model P-9D2C-AA72 or later.
(*5) Please upgrade the version to 07-00-/A of the succeeding model P-242C-AB77 or later.
(*6) Please upgrade the version to 07-00-/B of the succeeding model P-242C-AC77 or later.
(*7) Please upgrade the version to 07-00-/B of the succeeding model P-1B2C-AC72 or later.
(*8) Please upgrade the version to 07-00-/B of the succeeding model P-1M2C-AC72 or later.
(*9) Please upgrade the version to 07-00-/B of the succeeding model P-9D2C-AC72 or later.
(*10) Please upgrade the version to 07-00-/A of the succeeding model P-242C-AD77 or later.
(*11) Please upgrade the version to 07-00-/A of the succeeding model P-1B2C-AD72 or later.
(*12) Please upgrade the version to 07-00-/A of the succeeding model P-1M2C-AD72 or later.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, carry out the following workarounds:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the port that the NNM utility function of JP1/PFM - View uses.

Note that there is no workaround for JP1/PFM - Manager and the export and backup functions of JP1/PFM - Agent except for JP1/PFM - View.

Revision history

- February 4, 2008: Information about fixed versions and release time of 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 is updated.

- October 20, 2006: Information about fixed versions and release time of 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 is updated.
- April 26, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

©Hitachi, Ltd. 1994, 2008. All rights reserved.

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: April 26, 2006

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for JP1/Cm2/Network Node Manager

If JP1/Cm2/Network Node Manager (NNM) receives data unexpectedly through the port that snmpdm processing of NNM uses, a DoS (Denial of Service) might occur (due to snmpdm processing locking up CPU resources).
Fixed versions for the recent versions are available indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
JP1/Cm2/Network Node Manager	P-2442-6274	07-00 to 07-01-/B	Windows	07-10-04 (*3)	October 21, 2005	April 26, 2006
	P-9D42-6271	07-00 to 07-01-/B	Solaris	07-10-04 (*3)	October 21, 2005	April 26, 2006
JP1/Cm2/Network Node Manager 250	P-2442-6264	06-71-/D	Windows	06-71-SN	March 31, 2006	April 26, 2006
		06-00 to 06-71-/C		06-71-SN (*1)	March 31, 2006	April 26, 2006
	P-2442-6294	05-20 to 05-20-/F		(*4)		April 26, 2006
	P-9D42-6261	06-71-/C	Solaris	06-71-SF (*2)	March 31, 2006	April 26, 2006
		06-00 to 06-71-/B		06-71-SF (*1)(*2)	March 31, 2006	April 26, 2006
	P-9D42-6211	05-20 to 05-20-/E		(*4)		April 26, 2006
	P-2442-6164	06-71-/D		06-71-SN	March 31, 2006	April 26, 2006

JP1/Cm2/Network Node Manager Enterprise		06-00 to 06-71-/C	Windows	06-71-SN (*1)	March 31, 2006	April 26, 2006
	P-2442-6194	05-20 to 05-20-/F		(*4)		April 26, 2006
	P-9D42-6161	06-71-/C	Solaris	06-71-SF (*2)	March 31, 2006	April 26, 2006
		06-00 to 06-71-/B		06-71-SF (*1)(*2)	March 31, 2006	April 26, 2006
	P-9D42-6111	05-20 to 05-20-/E		(*4)		April 26, 2006
Cm2/Network Node Manager Unlimited	P-2442-5194	05-00 to 05-00-/A	Windows	(*4)		April 26, 2006
Cm2/Network Node Manager Enterprise	P-1642-511	05-00	HI-UX/WE2	(*4)		April 26, 2006
Cm2/Network Node Manager 250	P-2442-5294	05-00 to 05-00-/A	Windows	(*4)		April 26, 2006
	P-1642-521	05-00	HI-UX/WE2	(*4)		April 26, 2006

(*1) Please upgrade to the latest revision (that is, 06-71-/D for Windows, and 06-71-/C for Solaris), and then apply the corrective patch.
Note that products that operate while linked to NNM might also have to be upgraded. For details on the appropriate version of each linked product, refer to the applicable documentation for that product (such as Readme files or documentation provided with the software).

(*2) If NNM and JP1/Cm2/Extensible SNMP Agent (ESA) are installed on different machines, please apply the corrective patches indicated below. (If NNM and ESA are both installed on the same machine, no corrective patches are necessary.)

- 06-71-SF (patch for model P-9D42-6261 and P-9D42-6161)

(*3) Please upgrade to the latest revision. (If your NNM version is between 07-10 and 07-10-03, no upgrade is necessary.)
Note that products that operate while linked to NNM might also have to be upgraded. For details on the appropriate version of each linked product, refer to the applicable documentation for that product (such as Readme files or documentation provided with the software).

(*4) For detailed information about this model, contact your Hitachi support service representative.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, carry out the following workarounds:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the port that NNM uses.

Revision history

- April 26, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

| Term of Use | Privacy Notice | About Hitachi |

©Hitachi, Ltd. 1994, 2008. All rights reserved.

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: April 26, 2006

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for System Manager and JP1/Server Conductor

If System Manager and JP1/Server Conductor receive a large volume of invalid packet data, the manager service might stop.
Fixed versions for the recent versions are available indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
JP1/Server Conductor/Blade Server Manager	P-2418-6271	07-50, 07-50-/A, 07-51, 07-53, 07-55	Windows	07-63	March 3, 2006	April 26, 2006
	P-2418-3B6X	07-50, 07-50-/A, 07-51, 07-53, 07-55		(*1)		April 26, 2006
JP1/Server Conductor/Server Manager	P-2418-6371	07-50		07-50-/A	March 14, 2006	April 26, 2006
Server Conductor/Blade Server Manager	P-2418-6261	06-00, 06-00-/A		(*2)		April 26, 2006
Server Conductor/Server Manager	P-2418-6361	06-00, 06-00-/A		(*3)		April 26, 2006
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		05-52-/D	March 31, 2006	April 26, 2006
		05-00,				

	P-2418-315U	05-10, 05-20, 05-21, 05-30, 05-50-/A, 05-52-/A, 05-52-/B, 05-52-/C		05-52-/D	March 31, 2006	April 26, 2006
System Manager - Management Console Version 3.0	P-2418-3134	03-00, 03-00-/A, 03-10, 03-20, 03-30, 03-30-/A, 03-31-/A, 03-40, 03-42, 03-44-/A, 03-50, 03-60, 03-60-/A, 03-60-/C, 03-60-/D		(*4)		April 26, 2006

(*1) Please upgrade the version to 07-63 of model P-2418-6271 or later.
(*2) Please upgrade the version to 07-63 of succeeding model P-2418-6271 or later.
(*3) Please upgrade the version to 07-50-/A of succeeding model P-2418-6371 or later.
(*4) Please upgrade the version to 05-52-/D of succeeding model P-2418-3154 or later.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, carry out the following workarounds:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the ports that System Manager and JP1/Server Conductor/Blade Server Manager use.

Revision history

- April 26, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-

Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.

- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

©Hitachi, Ltd. 1994, 2008. All rights reserved.

Update: April 26, 2006

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for JP1/File Access Control

If JP1/File Access Control (JP1/FAC) receives data unexpectedly, a DoS (Denial of Service) might occur. Until the JP1/FAC server is rebooted, server processing might be disabled.
Fixed versions for the recent versions are available indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
JP1/File Access Control	P-1B2C-7A71	07-01	HP-UX	07-01-/A	March 31, 2006	April 26, 2006
	P-1B2C-7A61	06-72-A, 06-72-B		(*1)		April 26, 2006
	P-242C-7A74	07-00-/A	Windows	07-00-/B	March 31, 2006	April 26, 2006
	P-242C-7A64	06-72, 06-72-/B		(*2)		April 26, 2006

(*1) Please upgrade the version to 07-01-/A of succeeding model P-1B2C-7A71 or later.
(*2) Please upgrade the version to 07-00-/B of succeeding model P-242C-7A74 or later.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]

Until the fixed modules are applied, carry out the following workarounds:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the port that JP1/FAC uses.

Revision history

- April 26, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

©Hitachi, Ltd. 1994, 2008. All rights reserved.

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: April 26, 2006

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for JP1/Security Integrated Manager

If JP1/Security Integrated Manager (JP1/SCIM) receives requests unexpectedly, the connection between server and client might be disabled, and the services that JP1/SCIM provides (log collection service, etc.) might not be supplied.
Fixed versions for the recent versions are available indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
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	March 31, 2006	April 26, 2006
JP1/Security Integrated Manager	P-9D2C-7761	06-72, 06-73, 06-73-/A		06-73-/B	March 31, 2006	April 26, 2006

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]

Until the fixed modules are applied, carry out the following workarounds:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the port that JP1/SCIM uses.

Revision history

- April 26, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

©Hitachi, Ltd. 1994, 2008. All rights reserved.

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: June 20, 2006

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for JP1/Server Conductor/Deployment Manager

If JP1/Server Conductor/Deployment Manager receives a large volume of invalid packet data, the following services might stop or be disabled. Until all services of JP1/Server Conductor/Deployment Manager are rebooted, these services might be disabled.

- Deployment Manager for DPM
- Service Client for DPM (Windows/Linux)

The fixed versions that are available for the recent versions are indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
JP1/Server Conductor /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 (*2)	07-54-/A, 07-55-/A, 07-56	May 31, 2006	June 20, 2006
JP1/Server Conductor /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	May 31, 2006	June 20, 2006
Server Conductor /Deployment Manager	R-1V15-11733A	01-00, 01-01, 06-00, 06-00-/A		(*1)		June 20, 2006

(*1) Please upgrade the version to 07-54-/A, 07-55-/A or 07-56 of the succeeding model (R-1V15-12287A).

(*2) These products are bundled with Service Client for DPM for use on both Windows and Linux platforms.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, carry out the following workaround:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the ports that JP1/Server Conductor/Deployment Manager uses.

Revision history

- June 20, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

©Hitachi, Ltd. 1994, 2008. All rights reserved.

Update: October 20, 2006

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for JP1/Cm2 hierarchical management products

If JP1/Cm2/Hierarchical Agent or JP1/Cm2/SubManager receives invalid packet data, a DoS (Denial of Service) might occur. If this happens, you need to restart the OS.
The fixed versions that are available for the recent versions are indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
JP1/Cm2/Hierarchical Agent	P-2442-6Y74	07-00 to 07-00-/B	Windows (x86)	07-10-10	August 1, 2006	October 20, 2006
		07-10 to 07-10-/A				October 20, 2006
	P-2442-6Y64	06-00 to 06-00-/B		06-71-/B	September 11, 2006	October 20, 2006
		06-51 to 06-51-/A				October 20, 2006
		06-71 to 06-71-/A				October 20, 2006
	P-2442-6Y94	05-20		(*1)		October 20, 2006
		05-21				October 20, 2006
	P-2442-5Y94	05-00				October 20, 2006
	P-2442-6B74	07-00 to 07-00-/A		07-10-/A	August 9, 2006	October 20, 2006
		07-10 to 07-10				October 20, 2006
	P-2442-6B64	06-00 to 06-00-/B		06-71-/A	September 11, 2006	October 20, 2006
		06-51 to 06-51-/A				October 20, 2006
		06-71				October 20, 2006

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

JP1/Cm2/SubManager	P-2442-6C64	06-00 to 06-00-/B		06-71-/A	September 11, 2006	October 20, 2006
		06-51 to 06-51-/A				October 20, 2006
		06-71				October 20, 2006
	P-2442-6D64	06-00 to 06-00-/B		06-71-/A	September 11, 2006	October 20, 2006
		06-51 to 06-51-/A				October 20, 2006
		06-71				October 20, 2006
	P-2442-5B94	05-00 to 05-00-/A		(*2)		October 20, 2006
		05-20 to 05-20-/B				October 20, 2006
	P-2442-5C94	05-00 to 05-00-/A		(*3)		October 20, 2006
		05-20 to 05-20-/B				October 20, 2006
	P-2442-5D94	05-00 to 05-00-/A		(*4)		October 20, 2006
		05-20 to 05-20-/B				October 20, 2006

(*1) Please upgrade the version to 06-71-/B of the succeeding model P-2442-6Y64 or later, or upgrade to version 07-10-10 of the succeeding model P-2442-6Y74 or later.

(*2) Please upgrade the version to 06-71-/A of the succeeding model P-2442-6B64 or later, or upgrade to version 07-10-/A of the succeeding model P-2442-6B74 or later.

(*3) Please upgrade the version to 06-71-/A of the succeeding model P-2442-6C64 or later, or upgrade to version 07-10-/A of the succeeding model P-2442-6B74 or later.

(*4) Please upgrade the version to 06-71-/A of the succeeding model P-2442-6D64 or later, or upgrade to version 07-10-/A of the succeeding model P-2442-6B74 or later.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, please carry out the following workaround:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the ports that JP1/Cm2 hierarchical management products use.

Revision history

- October 20, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

©Hitachi, Ltd. 1994, 2008. All rights reserved.

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: July 6, 2007

HS06-007;
Vulnerability of DoS in JP1 Products

Solutions for JP1/Base

If JP1/Base receives data unexpectedly through a port, the JP1/Base service might stop. Until the JP1/Base service is rebooted, event operations that use the JP1/Base event service might be disabled.
The fixed versions that are available for the recent versions are indicated below. Upgrade the JP1 version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
JP1/Base	P-9D2C-6L71	07-51 to 07-51-04	Solaris	07-51-05	May 15, 2006	November 8, 2006
		07-50 to 07-50-07		07-50-08	September 29, 2006	November 8, 2006
		07-11 to 07-11-08		07-11-09	August 28, 2006	November 8, 2006
		07-10 to 07-10-C1		07-10-/F	May 15, 2006	November 8, 2006
		07-00 to 07-00-D1		07-00-/G	July 28, 2006	November 8, 2006
	P-9D2C-6L61	06-71 to 06-71-/M		(*1)		November 8, 2006
		06-51 to 06-51-M2		(*1)		November 8, 2006
Job Management Partner 1/Base	P-9D2C-6L72	07-51		07-51-09	June 28, 2007	July 6, 2007
	P-9D2C-6L62	06-51 to 06-51-/F		(*1)		November 8, 2006
		06-71 to 06-71-/G		(*1)		November 8, 2006

(*1) For detailed information about this model, contact your Hitachi support service representative.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, please carry out the following workaround:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the ports that JP1/Base uses.

Revision history

- July 6, 2007: Information about fixed versions of P-9D2C-6L72 is updated.
- November 8, 2006: Information about vulnerability of DoS in JP1 products is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

©Hitachi, Ltd. 1994, 2008. All rights reserved.