Software Vulnerability Information
Software Division

HITACHI
Inspire the Next

Search in the Hitachi site by Google

> GO

> Advanced search

Update: March 30, 2007

DoS Vulnerability in HiRDB Datareplicator

- Affected products

Corrective action	Product name	Platform	Last update
HS06-023-01	HiRDB Datareplicator	Windows, Windows(IPF), AIX, Linux, Linux(IPF), HP-UX, HP-UX(IPF), Solaris, HI-UX/WE2	March 30, 2007

- Problem description

A DoS (Denial of Service) vulnerability was found in the above products.

Revision history

- March 30, 2007: Corrective actions page is updated.
- January 24, 2007: 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

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.

HIRT Hitachi Incident Response Team

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

Software Vulnerability Information
Software Division

HITACHI
Inspire the Next

| Home | Software | ≫ Security |

Home > Vulnerability Information > Software Vulnerability Information > HS06-023-01

Search in the Hitachi site by Google

> GO

> Advanced search

> 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: March 30, 2007

HS06-023;
DoS Vulnerability in HiRDB Datareplicator

Solutions for HiRDB Datareplicator

If HiRDB Datareplicator receives data unexpectedly, a DoS (Denial of Service) might occur due to domination of CPU resources. In this case, restart the OS. The fixed versions available for existing versions are indicated below. Upgrade the HiRDB 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-2462-1K74	07-04 to 07-04-02	Windows	07-04-03	October 2, 2006	January 24, 2007
		07-00 to 07-01-/F		07-01-/G	September 9, 2006	January 24, 2007
	P-2462-1K77	07-00 to 07-01		(*1)		January 24, 2007
	P-2862-1K74	07-04 to 07-04-02	Windows (IPF)	07-04-03	October 2, 2006	January 24, 2007
		07-01 to 07-01-/D		07-01-/G	September 9, 2006	January 24, 2007
	P-1M62-1K71	07-04	AIX	07-04-03	October 2, 2006	January 24, 2007
		07-00 to 07-03		(*1)		January 24, 2007
	P-9S62-1K71	07-04	Linux	07-04-03	October 2, 2006	January 24, 2007
		07-00 to 07-03		(*1)		January 24, 2007
						March

HiRDB Datareplicator Version 7			06-03 to 06-03-/F		06-03-/M	January 9, 2007	30, 2007
	P-9V62-1K71	07-04	Linux (IPF)	07-04-03	October 2, 2006	January 24, 2007
		07-01 to 07-03		(*1)		January 24, 2007
	P-1B62-1K71	07-04	HP-UX	07-04-03	October 2, 2006	January 24, 2007
		07-00 to 07-02		(*1)		January 24, 2007
	P-1J62-4K71	07-04	HP-UX (IPF)	07-04-03	October 2, 2006	January 24, 2007
		07-01 to 07-02		(*1)		January 24, 2007
	P-9D62-1K71	07-04	Solaris	07-04-03	October 2, 2006	January 24, 2007
		07-00 to 07-01		(*1)		January 24, 2007
	P-1662-1K7	07-00	HI-UX/WE2	(*1)		January 24, 2007
HiRDB Datareplicator Version 7(64)	P-1M62-4K71	07-04	AIX	07-04-03	October 2, 2006	January 24, 2007
		07-00 to 07-03		(*1)		January 24, 2007
	P-1B62-4K71	07-04	HP-UX	07-04-03	October 2, 2006	January 24, 2007
		07-00 to 07-02		(*1)		January 24, 2007
	P-9D62-4K71	07-04	Solaris	07-04-03	October 2, 2006	January 24, 2007
		07-00 to 07-01		(*1)		January 24, 2007
	P-2462-1K64	06-03 to 06-03-/L	Windows	06-03-/M	January 17, 2007	March 30, 2007
		06-00 to 06-01-/G		(*1)		January 24, 2007
	P-2462-1K67	06-01		(*1)		January 24, 2007
		06-03 to			January 9,	March

Product	Model	Version	OS			End date
HiRDB Datareplicator Version 6	P-1M62-1K61	06-03-/K	AIX	06-03-/M	2007	30, 2007
		06-00 to 06-01-/E		(*1)		January 24, 2007
	P-9S62-1K61	06-00	Linux	(*1)		January 24, 2007
	P-1B62-1K61	06-03 to 06-03-/J	HP-UX	06-03-/M	January 9, 2007	March 30, 2007
		06-00 to 06-02		(*1)		January 24, 2007
	P-9D62-1K61	06-00 to 06-01	Solaris	(*1)		January 24, 2007
	P-1662-1K6	06-00 to 06-01	HI-UX/WE2	(*1)		January 24, 2007
HiRDB Datareplicator Version 6(64)	P-1M62-4K61	06-03 to 06-03-/H	AIX	06-03-/M	January 9, 2007	March 30, 2007
		06-01 to 06-01-/E		(*1)		January 24, 2007
	P-1B62-4K61	06-03 to 06-03-/J	HP-UX	06-03-/M	January 9, 2007	March 30, 2007
		06-00 to 06-02		(*1)		January 24, 2007
	P-9D62-4K61	06-00 to 06-01	Solaris	(*1)		January 24, 2007
HiRDB Datareplicator Version 5.0	P-2462-4K54	05-00 to 05-03-/G	Windows	(*1)		January 24, 2007
	P-9S62-1K11	05-03	Linux	(*1)		January 24, 2007
	P-1B62-1K11	05-00 to 05-03-/H	HP-UX	(*1)		January 24, 2007
	P-9D62-1K11	05-02 to 05-03-/A	Solaris	(*1)		January 24, 2007
	P-1662-1K1	05-00 to 05-03-/F	HI-UX/WE2	(*1)		January 24, 2007
HiRDB Datareplicator Version 5.0(64)	P-1B62-4K51	05-01 to 05-03-/H	HP-UX	(*1)		January 24, 2007
	P-9D62-4K51	05-03	Solaris	(*1)		January 24, 2007
	P-2462-	02-00 to	Windows	(*1)		January 24,

Product name	Model	Version	Platform	Fixed version	Release time	Last update
	4K14	04-00-/P				2007
HiRDB Datareplicator	P-1B62-4K11	02-00 to 04-00-/G	HP-UX	(*1)		January 24, 2007
	P-1662-4K1	02-00 to 04-01-/L	HI-UX/WE2	(*1)		January 24, 2007

[Affected models, versions, and fixed versions bundled with HiRDB]

Please note that this vulnerability also affects HiRDB products that bundle HiRDB Datareplicator.

Product name	Model	Version	Platform	Fixed version	Release time	Last update
HiRDB/Single Server Version 7	P-2462-7174	07-03 to 07-03-13	Windows	07-03-14	November 9, 2006	January 24, 2007
		07-00 to 07-02-2K		07-02-2N	October 19, 2006	January 24, 2007
	P-2462-7177	07-00 to 07-02		(*1)		January 24, 2007
	P-2862-7174	07-03 to 07-03-13	Windows (IPF)	07-03-14	November 9, 2006	January 24, 2007
		07-01-/M to 07-02-2H		07-02-2Q	February 6, 2007	March 30, 2007
HiRDB/Parallel Server Version 7	P-2462-7374	07-03 to 07-03-13	Windows	07-03-14	November 9, 2006	January 24, 2007
		07-00 to 07-02-2L		07-02-2M	September 27, 2006	January 24, 2007
	P-2462-7377	07-00 to 07-02		(*1)		January 24, 2007
	P-2862-7374	07-03 to 07-03-13	Windows (IPF)	07-03-14	November 9, 2006	January 24, 2007
		07-01-/M to 07-02-2H		07-02-2Q	February 6, 2007	March 30, 2007
HiRDB/Single Server Version 6	P-2462-7164	06-00 to 06-02-3F		06-02-3G	February 15, 2007	March 30, 2007
HiRDB/Parallel Server Version 6	P-2462-7364	06-00 to 06-02-3E		06-02-3G	February 15, 2007	March 30, 2007
HiRDB/Workgroup Server Version 6	P-2462-8164	06-00 to 06-02-3E		06-02-3G	February 15, 2007	March 30, 2007
HiRDB/Single Server Version 5.0	P-2462-7154	05-02 to 05-06-/P	Windows	(*1)		January 24, 2007
	P-					January

HiRDB/Parallel Server Version 5.0	2462-7354	05-02 to 05-06-/P		(*1)	24, 2007
HiRDB/Single Server Workgroup Edition Version 5.0	P-2462-8154	05-05 to 05-06-/P		(*1)	January 24, 2007
HiRDB/Single Server 4.0	P-2462-7144	04-00 to 04-04-/B		(*1)	January 24, 2007
HiRDB/Parallel Server 4.0	P-2462-7344	04-00 to 04-04		(*1)	January 24, 2007

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

[Affected models (HiRDB product sets)]

Please note that this vulnerability also affects HiRDB product sets that contain HiRDB Datareplicator. Please upgrade the version of HiRDB Datareplicator in the following product sets. For details on the affected versions and fixed versions, contact your Hitachi support service representative.

Product set name	Model	Platform	Last update
HiRDB/Single Server Version 7	P-9S62-1173		January 24, 2007
HiRDB/Parallel Server Version 7	P-9S62-1373		January 24, 2007
HiRDB/Single Server Version 6	P-9S62-1163		January 24, 2007
HiRDB/Parallel Server Version 6	P-9S62-1363		January 24, 2007
HiRDB/Workgroup Server Version 6	P-9S62-2163	Linux	January 24, 2007
HiRDB/Single Server	P-9S62-1123		January 24, 2007
HiRDB/Parallel Server	P-9S62-1323		January 24, 2007
HiRDB/Single Server Workgroup	P-9S62-2123		January 24, 2007

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 HiRDB Datareplicator uses.

Revision history

- March 30, 2007: Information about fixed versions and release time of P-9S62-1K71, P-2462-1K64, P-1M62-1K61, P-1B62-1K61, P-1M62-4K61, P-1B62-4K61, P-2862-7174, P-2862-7374, P-2462-7164, P-2462-7364, and P-2462-8164 is updated.
- January 24, 2007: Information about DoS vulnerability in HiRDB Datareplicator 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