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 8, 2004

Buffer Overrun of the MDAC Function

- Affected product

Corrective actions	Product name	Platform	Last update
HS04-001-01	HiRDB	Windows	April 8, 2004
HS04-001-02	AuditStage and Quality Manager	Windows	April 8, 2004
HS04-001-03	DBPARTNER ODBC Driver, DABroker for ODBC, DBPARTNER2, and HITSENSER5	Windows	April 8, 2004

- Problem description

  On January 13, 2004, Microsoft announced the vulnerability of the buffer overrun of the Microsoft Data Access Components (MDAC) function (MS04-003).

  This is a problem because an attacker who successfully exploits this vulnerability can gain the same level of privileges over the system as the program that initiated the broadcast request.
  The above products include MDAC. If you are using them, please refer to Microsoft Web site and replace MDAC with a new version.

Revision history

- April 8, 2004: This page is released.

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

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 8, 2004

HS04-001;
Buffer Overrun of the MDAC Function

Solution for HiRDB

In HiRDB, the problem was found that buffer overrun of the MDAC function could allow code execution.

[Influence]

When installing HiRDB/Run Time Version 7 (*1) or HiRDB/Developer's Kit Version 7, MDAC 2.6 Service Pack1 is copied in *HiRDB-installation-directory*`\url` only if you selected the ODBC Driver with custom-installation. If the version of the ODBC Driver on the installation target machine is old, we ask customers to install this copied MDAC to use HiRDB. This is the case in which the problem occurs.

(*1)HiRDB/Run Time Version 7 included in HiRDB/Single Server Version 7 or HiRDB/Parallel Server Version 7 is also affected.

Model	Product name	Version	Platform
P-2662-1174	HiRDB/Run Time Version 7	07-00	Windows
P-2662-1274	HiRDB/Developer's Kit Version 7	07-00	
P-2462-7174	HiRDB/Single Server Version 7	07-00	
P-2462-7374	HiRDB/Parallel Server Version 7	07-00	

If you have installed the MDAC delivered by the above products, please replace it following the Microsoft Web site. Also, please delete MDAC 2.6 Service Pack1 copied in *HiRDB-installation-directory*`\url`.

Revision history

- April 8, 2004: Information about MDAC problem relating to HiRDB 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 |

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 8, 2004

HS04-001;
Buffer Overrun of the MDAC Function

Solution for AuditStage and Quality Manager

In AuditStage and Quality Manager, the problem was found that buffer overrun of the MDAC function could allow code execution. MDAC included in the following products has this problem.

[Influence]

Your system is affected by this problem only when you have installed MDAC included in AuditStage or Quality Manager.

Model	Product name	Version	Platform
RT-1V37-QA1W	AuditStage	07-01	Windows
RT-12463-9D14	Quality Manager (Additional)	04-82	
RT-12463-9E14	Quality Manager 2User	04-82	
RT-12463-9Q14	Prism Quality Manager for HiRDB	01-00-/B	
RT-12463-9S14	Prism Quality Manager for Oracle	01-00-/B	

If you have installed the MDAC that is delivered by the above products, please replace it following the Microsoft Web site.

Revision history

- April 8, 2004: Information about MDAC problem included in AuditStage and Quality Manager is released.

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

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 8, 2004

HS04-001;
Buffer Overrun of the MDAC Function

Solution for DBPARTNER ODBC Driver, DABroker for ODBC, DBPARTNER2, and HITSENSER5

In DBPARTNER ODBC Driver, DABroker for ODBC, DBPARTNER2 and HITSENSER5, the problem was found that buffer overrun of the MDAC function could allow code execution.

[Influence]

When installing DBPARTNER ODBC Driver/DBPARTNER ODBC 3.0 Driver, the MDAC 2.5 installation form module is copied only if you selected "MDAC 2.5" with custom-installation. In the case of DABroker for ODBC, the MDAC 2.5 installation form module is copied as standard. If the version of the ODBC Driver on the installation target machine is old, we ask customers to install this copied MDAC to use these products. This is the case in which the problem occurs. The DBPARTNER ODBC Driver included in the following DBPARTNER2 and HITSENSER5-related products also have this problem.

Model	Product name	Version	Platform
P-2663-5514	DBPARTNER ODBC Driver	01-06 - 01-10-/B	Windows
P-2663-5614	DBPARTNER ODBC 3.0 Driver	01-00 - 01-03	
P-F2463-21546	DABroker for ODBC	01-00 - 01-02	
P-2663-4514	DBPARTNER2 Client	01-05 - 01-11-/B	
P-2663-4614	DBPARTNER2 Client	01-05 - 01-11-/B	
P-2663-4714	DBPARTNER2 Client	01-05 - 01-11-/B	
P-2663-6514	DBPARTNER2 Client	01-05 - 01-11-/B	
P-2663-6614	DBPARTNER2 Client	01-05 - 01-11-/B	
P-2663-6714	DBPARTNER2 Client	01-05 - 01-11-/B	
P-2463-2194	DBPARTNER2 COBOL Components	01-00 - 01-00-/A	
P-2463-2614	DBPARTNER2 Multiuser Option	01-00	
P-2663-1P14	HITSENSER5 Professional for Cosmicube	01-00 - 02-40	
P-2663-1S14	HITSENSER5 Standard for Cosmicube	01-00 - 02-40	
P-2663-2P14	HITSENSER5 Professional for RDB	01-10 - 02-40	
P-2663-2S14	HITSENSER5 Standard for RDB	01-10 - 02-40	
P-2663-3P14	HITSENSER5 Professional	01-10 - 02-40	

P-2663-3S14	HITSENSER5 Standard	01-10 - 02-40
P-2463-3W14	HITSENSER5 Web	01-10 - 02-40
P-2463-CW14	HITSENSER5 Web	01-10 - 02-40

If you have installed the MDAC delivered by the above products, please replace it following the Microsoft Web site.

Revision history

- April 8, 2004: Information about the MDAC problem relating to DBPARTNER ODBC Driver, DABroker for ODBC, DBPARTNER2 and HITSENSER5 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