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

Vulnerability in the MDAC Function Could Allow Remote Code Execution

- Affected product

Corrective actions	Product name	Platform	Last update
HS06-013-01	DBPARTNER ODBC Driver, DABroker for ODBC, DBPARTNER2, HITSENSER5	Windows	June 20, 2006

- Problem description

On April 11, 2006, Microsoft released a security bulletin (MS06-014) about a vulnerability found in the Microsoft Data Access Components (MDAC) function, which could allow an attacker to execute codes remotely.
If the MDAC installation module is installed in the above products, see the Microsoft Web site, and then replace it with the latest MDAC version.

Revision history

- June 20, 2006: This page is released.

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: June 20, 2006

HS06-013;
Vulnerability in the MDAC Function Could Allow Remote Code Execution

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

A vulnerability that could allow an attacker to execute code remotely was discovered in the Microsoft Data Access Components (MDAC) function included in DBPARTNER ODBC Driver, DABroker for ODBC, DBPARTNER2, and HITSENSER5.

[Affected MDAC version]

This vulnerability is in the MDAC 2.5 installation module. The MDAC 2.5 installation module is copied (i) if "MDAC 2.5" is selected in a custom installation of DBPARTNER ODBC Driver/DBPARTNER ODBC 3.0 Driver, or (ii) in a default installation of DABroker for ODBC, or (iii) in an upgrade installation of MDAC 2.5 on a target machine.
This vulnerability is also in the DBPARTNER ODBC Driver included in the following DBPARTNER2 and HITSENSER5 related products.

[Affected models and versions]

Model	Product name	Version	Platform	Last update
P-2663-5514	DBPARTNER ODBC Driver	01-06 to 01-11		June 20, 2006
P-2663-5614	DBPARTNER ODBC 3.0 Driver	01-00 to 01-03		June 20, 2006
P-F2463-21546	DABroker for ODBC	01-00 to 01-02		June 20, 2006
P-2663-4514	DBPARTNER2 Client	01-05 to 01-12		June 20, 2006
P-2663-4614	DBPARTNER2 Client	01-05 to 01-12		June 20, 2006
P-2663-4714	DBPARTNER2 Client	01-05 to 01-12		June 20, 2006
P-2663-6514	DBPARTNER2 Client	01-05 to 01-12		June 20, 2006
P-2663-6614	DBPARTNER2 Client	01-05 to 01-12		June 20, 2006
		01-05 to		June 20,

P-2663-6714	DBPARTNER2 Client	01-12	Windows	2006
P-2463-2194	DBPARTNER2 COBOL Components	01-00 to 01-00-/A		June 20, 2006
P-2463-2614	DBPARTNER2 Multiuser Option	01-00 to 01-01		June 20, 2006
P-2463-8614	DBPARTNER2 Client for Jichitai	01-00		June 20, 2006
P-2663-1P14	HITSENSER5 Professional for Cosmicube	01-00 to 02-80		June 20, 2006
P-2663-1S14	HITSENSER5 Standard for Cosmicube	01-00 to 02-80		June 20, 2006
P-2663-2P14	HITSENSER5 Professional for RDB	01-10 to 02-80		June 20, 2006
P-2663-2S14	HITSENSER5 Standard for RDB	01-10 to 02-80		June 20, 2006
P-2663-3P14	HITSENSER5 Professional	01-10 to 02-80		June 20, 2006
P-2663-3S14	HITSENSER5 Standard	01-10 to 02-80		June 20, 2006
P-2463-3W14	HITSENSER5 Web CPU license	01-10 to 02-80		June 20, 2006
P-2463-CW14	HITSENSER5 Web connection license	01-10 to 02-80		June 20, 2006

If the MDAC installation module (version 2.5) is installed in the above products, see the Microsoft Web site, and then replace it with the latest MDAC version.

Revision history

- June 20, 2006: Information about vulnerability in the MDAC function could allow remote code execution is released.

Page Top

| Term of Use | Privacy Notice | About Hitachi |