Software Vulnerability Information
Software Division

Home > Vulnerability Information > Software Vulnerability Information > HS05-026

Update: January 20, 2006

SQL Injection Vulnerability in HITSENSER Data Mart Server

- Affected products

Corrective action	Product name	Platform	Last update
HS05-026-01	HITSENSER Data Mart Server/BS, HITSENSER Data Mart Server/BS-S, HITSENSER Data Mart Server/BS-M, HITSENSER Data Mart Server/BS-L, HITSENSER Data Mart Server/EX	Windows	January 20, 2006

- Problem description

The SQL injection vulnerability was found in the above products.
A malicious remote user can exploit this vulnerability to execute arbitrary SQL commands.

Revision history

- January 20, 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.

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

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

Update: January 20, 2006

HS05-026;
SQL Injection Vulnerability in HITSENSER Data Mart Server

Solution for HITSENSER Data Mart Server

A vulnerability was found where user authentication might be bypassed when using a configuration function in HITSENSER Data Mart Server.
Fixed versions are available for the versions indicated below. Please upgrade the HITSENSER 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
HITSENSER Data Mart Server/BS	C-7120-202	01-00 - 01-06	Windows	01-06-/A	November 30, 2005	January 20, 2006
HITSENSER Data Mart Server/BS-S	C-7120-212	01-00 - 01-06		01-06-/A	November 30, 2005	January 20, 2006
HITSENSER Data Mart Server/BS-M	C-7120-222	01-00 - 01-06		01-06-/A	November 30, 2005	January 20, 2006
HITSENSER Data Mart Server/BS-L	C-7120-232	01-00 - 01-06		01-06-/A	November 30, 2005	January 20, 2006
HITSENSER Data Mart Server/EX	C-7120-242	01-00 - 01-06		01-06-/A	November 30, 2005	January 20, 2006

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

Revision history

- January 20, 2006: Information about SQL Injection Vulnerability in HITSENSER Data Mart Server 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-

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

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