Software Vulnerability Information
Software Division

HITACHI
Inspire the Next

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.

Update: February 13, 2006

Cross-site Scripting and SQL Injection Vulnerabilities in Hitachi Business Logic - Container

- Affected products

Corrective action	Product name	Platform	Last update
HS06-002-01	Hitachi Business Logic - Container	Windows, Linux	February 13, 2006

- Problem description

Cross-site scripting and SQL injection vulnerabilities were found in the above products.
A malicious remote user can exploit these vulnerabilities to execute invalid scripts and execute arbitrary SQL commands.

Revision history

- February 13, 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

| Home | Software | » Security |

Japanese

Search in the Hitachi site by Google
GO
> Advanced search

Home > Vulnerability Information > Software Vulnerability Information > HS06-002-01

Update: February 13, 2006

HS06-002;
Cross-site Scripting and SQL Injection Vulnerabilities in Hitachi Business Logic - Container

Solutions and Notes for Hitachi Business Logic - Container

Cross-site scripting and SQL injection vulnerabilities were found in the extended receiving box function of Hitachi Business Logic - Container (BLC). Take the corrective action indicated below.
If your system uses the API (application program interface) provided by BLC, also see the note.

[Corrective Action]

Fixed versions containing countermeasures against the vulnerabilities in the extended receiving box function of BLC are available for the versions indicated below. Upgrade the BLC version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name (*1)	Model	Version	Platform	Fixed version	Release time	Last update
Hitachi Business Logic - Container	P-2443-9114	02-03 to 03-00-/B	Windows	03-01	January 31, 2006	February 13, 2006
	P-9S43-9111	03-00 to 03-00-/B	Linux	03-01	January 31, 2006	February 13, 2006

(*1) This product is a component of the following product sets:

[Models of product sets]

Product set name	Models	Platform
Electronic Form Workflow - Professional Library Set	P-24Z4-GT64	Windows
	P-24Z4-G464	
Electronic Form Workflow - Entry Set	P-24Z4-GF54	
	P-24Z4-GF64	
	P-24Z4-G164	
Electronic Form Workflow - Entry Set Plus	P-24Z4-G664	
Electronic Form Workflow - Entry Set Plus Developer's Kit	P-24Z4-G764	

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

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Electronic Form Workflow - Professional Library Set	P-9SZ4-G461	Linux
Electronic Form Workflow - Entry Set	P-9SZ4-G161	
Electronic Form Workflow - Entry Set Plus	P-9SZ4-G661	
Electronic Form Workflow - Entry Set Plus Developer's Kit	P-9SZ4-G761	

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

[Note]
BLC does not execute escape processing internally to replace meta-characters contained in external API parameters. Therefore, if your system needs such escape processing for security, you must design user programs to execute such escape processing.
For details about this note, contact your Hitachi support service representative.

Revision history

- February 13, 2006: Information about cross-site scripting and SQL injection vulnerabilities in Hitachi Business Logic - Container 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