

Software Vulnerability Information

Software Division



[Home](#) | [Software](#) | [Security](#)

[Japanese](#)

Search in the Hitachi site by Google



[Advanced search](#)

[Home](#) > [Vulnerability Information](#) > [Software Vulnerability Information](#) > [HS05-025](#)

[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](#)



Update: December 27, 2005

Multiple Vulnerabilities of Hitachi Business Logic - Container

- Affected products

Corrective action	Product name	Platform	Last update
HS05-025-01	Hitachi Business Logic - Container	Windows, AIX	December 27, 2005

- Problem description

Multiple vulnerabilities were found in the above products. A malicious remote user can exploit these vulnerabilities to execute invalid scripts, execute arbitrary SQL commands, and cause HTTP Response Splitting.

Revision history

- December 27, 2005: 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.

Software Vulnerability Information

Software Division



Update: December 27, 2005

HS05-025;
Multiple Vulnerabilities of Hitachi Business Logic - Container

Solutions for Hitachi Business Logic - Container

The following vulnerabilities were found in Hitachi Business Logic - Container (BLC).

- Cross-site scripting

Invalid scripts might be executed on a browser because of invalid scripts sent through an input form.

- SQL Injection

SQL Injection might occur because of invalid SQL commands sent through an input form.

- HTTP Response Splitting

HTTP Response Splitting might occur because of invalid HTTP requests sent through an input form.

Fixed versions 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	01-00 - 02-06	Windows	03-00	September 6, 2005	December 27, 2005
	P-1M43-9111	01-01 - 02-00	AIX	(*2)		December 27, 2005

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

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

[Models of product sets]

--	--	--

> 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



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	

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

Revision history

- December 27, 2005: Information about multiple vulnerabilities of 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](#)