

# Software Vulnerability Information

## Software Division



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

[Japanese](#)

Search in the Hitachi site by Google



[Advanced search](#)

[Home](#) > [Vulnerability Information](#) > [Software Vulnerability Information](#) > HS04-006

Update: June 22, 2005

### Cached content replacement problem in Cosminexus Portal Framework

- Affected product

Corrective actions	Product name	Platform	Last update
HS04-006-01	Cosminexus Portal Framework	Windows, HP-UX, AIX, Solaris	June 22, 2005

- Problem description

In a portal web site using the above product, the content cached in a portlet that uses the <ut : cache> tag library to cache content may be replaced by other content. For example, when personal information is held in the cache, this problem could cause another user's information to be displayed.

#### Revision history

- June 22, 2005: Corrective actions page is updated.
- September 7, 2004: 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

[TOP](#)

[What's New](#)

[Notifications](#)

[Alert](#)

[Software Vulnerability Information](#)

[Links to Security Organizations](#)

[Email](#)  
[soft-security@itg.hitachi.co.jp](mailto: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](#)



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](#)

# Software Vulnerability Information

## Software Division



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

[» Japanese](#)

Search in the Hitachi site by Google

[» Advanced search](#)

[Home](#) > [Vulnerability Information](#) > [Software Vulnerability Information](#) > [HS04-006-01](#)

Update: June 22, 2005

**HS04-006;**  
**Cached content replacement problem in Cosminexus Portal Framework**

### Solution for Cosminexus Portal Framework

A security problem in the portal web site of Cosminexus Portal Framework was found. If you use or will use the <ut : cache> tag library, please apply the fixed version below to your system.

#### [Affected models, versions and fixed versions]

Model	Product name	Version	Platform	Fixed version	Release Time	Last Update
P-2443-3314	Cosminexus Portal Framework	01-00, 01-00-/A, 01-01	Windows	01-02-/A (*1)	August 30, 2004	September 7, 2004
		01-02		01-02-/A	August 30, 2004	September 7, 2004
		02-00, 02-00-/A, 02-01		02-02-/C (*1)	August 30, 2004	September 7, 2004
		02-02 - 02-02-/B		02-02-/C	August 30, 2004	September 7, 2004
		02-03 - 02-03-/C		02-03-/D	August 30, 2004	September 7, 2004
P-1M43-3314		01-00	AIX	01-02-/B (*1)	August 30, 2004	September 7, 2004
		01-02, 01-02-/A		01-02-/B	August 30, 2004	September 7, 2004
		02-00, 02-01		02-02-/D (*1)	August 30, 2004	September 7, 2004
		02-02 - 02-02-/C		02-02-/D	August 30, 2004	September 7, 2004
P-1B43-3314		01-00	HP-UX	01-00-/A	August 30, 2004	September 7, 2004
	02-00	02-02-/A (*1)		August 30, 2004	September 7, 2004	
	02-02	02-02-/A		August 30, 2004	September 7, 2004	
P-9D43-3314		01-00	Solaris	(*2)	June 22, 2005	

[» TOP](#)

[» What's New](#)

[» Notifications](#)

[» Alert](#)

[» Software Vulnerability Information](#)

[» Links to Security Organizations](#)

[» Email](#)  
[soft-security@itg.hitachi.co.jp](mailto: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](#)



(\*1) Please upgrade the version to a fixed revision.

(\*2) For the fixed versions, contact your Hitachi support service representative.

**[Affected models, versions and fixed versions of products]**

Product set		Affected components						
Model	Cosminexus Portal Framework products	Model	Component name	Version	Platform	Fixed version	Release Time	Last Update
P-24Z4-3514	Cosminexus Portal Framework entry set500	P-2443-3414	Cosminexus Portal Framework Light	02-00	Windows	02-00-/A	August 30, 2004	September 7, 2004
P-24Z4-3614	Cosminexus Portal Framework entry set1000							
P-24Z4-3714	Cosminexus Portal Framework entry set2000							

To replace the affected components in the products above with fixed versions, please contact us for a reorder.

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

**[Provisional Workaround]**

The following provisional workaround exists for this vulnerability. Please implement this provisional workaround until you apply the fixed version. Edit the setup so that access to the portlet using the <ut : cache> tag library is forbidden.

Please refer to the manual for the setup.

Model	Version	Manual in Japanese Version
P-2443-3314, P-1M43-3314, P-1B43-3314, P-9D43-3314, P-24Z4-3514, P-24Z4-3614, P-24Z4-3714, P-2443-3414	01-00 - 02-02	Appendix B.3 The permission in the definition file (AccessControl.xml)
	02-03	7.4.3 specified portlet - (1) portlet of permission of specify

When the above workaround is applied and the portlet of relevance has already been deployed on the portal by the end-user, the message "No permission for portlet" will appear on the portal and the portlet cannot be accessed. To enable access again, apply the fixed version, and then cancel the setup that forbids access to the portlet using the <ut : cache> tag library.

Revision history

- June 22, 2005: Information about fixed version and release time of P-9D43-3314 is updated.
- September 7, 2004: Information about a cached content replacement problem in Cosminexus Portal Framework 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](#)