

# Software Vulnerability Information

## Software Division



Update: March 22, 2005

## Non-response of Cosminexus Server Component Container for Java

- Affected products

Corrective action	Computer Associates Product name	Platform	Last update
<a href="#">HS05-006-01</a>	Cosminexus Server Component Container, Cosminexus Server Component Container for Java	Windows, HP-UX, AIX, Solaris	March 14, 2005

- Problem description

On March 14, 2005, US-CERT released their [Vulnerability Note VU#204710](#) about how Apache Tomcat fails to properly handle certain requests. Sending invalid data to the port for communication with web servers may cause denial of service of the web application servers that use the above products.

### Revision history

- March 22, 2005: The US-CERT information about this vulnerability is added.
- March 14, 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

> 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](#) > [HS05-006-01](#)

Update: March 14, 2005

**HS05-006;**

**Non-response of Cosminexus Server Component Container for Java**

### Solution for Cosminexus Server Component Container for Java

The following vulnerability was found in Cosminexus Server Component Container for Java that is included in Cosminexus Server - Standard Edition Version 4:

- Sending invalid data to the port for communication with web servers that use Cosminexus Server Component Container or Cosminexus Server Component Container for Java may cause denial of service of the web application servers.

A fixed version is available, so please apply the fixed version.

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

Product		Component						
Product name	Version	name	Model	Version	Platform	Fixed version	Release time	Last update
Cosminexus Server - Standard Edition Version 4	04-01	Cosminexus Server Component Container for Java	P-2443-8114	02-00 to 02-00-L	Windows	02-00-M	February 28, 2005	March 14, 2005
			P-1B43-8111		HP-UX	02-00-M	February 28, 2005	March 14, 2005
			P-9D43-8111		Solaris	02-00-M	February 28, 2005	March 14, 2005
		Cosminexus Server Component Container	P-1M43-8111		AIX	02-00-M	February 28, 2005	March 14, 2005

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

#### [Workarounds]

The following provisional workaround exists for this vulnerability. Please implement this provisional workaround until you apply the fixed version.

> [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](#)



Make the J2EE server communicate only with the machines authenticated using IP filtering. Do not use security diagnosis tool, .etc, to send invalid data to the port (port ajp12) used for communication with web servers.

## Revision history

- March 14, 2005: Information about non-response of Cosminexus Server Component Container for Java 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](#)