

Software Vulnerability Information

Software Division

HITACHI
Inspire the Next

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

» [Japanese](#)

Search in the Hitachi site by Google

> GO

> Advanced search

Home > Vulnerability Information > Software Vulnerability Information > HS02-010

Update: July 14, 2003

File Disclosure Vulnerability in Apache Tomcat

On September 24, 2002, a vulnerability in the file disclosure of Tomcat provided by Apache Software Foundation was announced ([Bugtraq-id: 5786](#)). The Cosminexus component Cosminexus Component Container uses Tomcat as a Web container, so this vulnerability also affects Cosminexus products.

The following table lists the products that have this vulnerability. This problem is addressed in the patch Cosminexus Component Container 05-00-SA provided for [Cross Site Scripting Vulnerability](#) announced on July 10, 2002. If you already applied the patch, you need not take any countermeasures. If you have not yet applied this patch, contact your Hitachi support service representative.

Models and versions of Cosminexus Component Container affected by the vulnerability

● Japanese version

Product			Component				Platform
Product name	Model	Version	Name	Model	Version	Version of patch	
Cosminexus Application Server Version 5	P-2443-1D54	05-00	Cosminexus Component Container	P-2443-8124	05-00	05-00-SA	Windows NT 4.0/2000
Cosminexus Developer Version 5	P-2443-1F54	05-00					

- This problem is corrected in the following products for Windows: Cosminexus Application Server Version 5 05-00-/A and later, and Cosminexus Developer Version 5 05-00-/A and later.
- This security problem does not affect the following products for AIX: Cosminexus Application Server Version 5 05-00 and Cosminexus Developer Version 5 05-00.

Revision history

- July 14, 2003: This page is revamped.

> [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](#)



- 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](#)