

# 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](#) > 
 HS06-004

> 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



Update: March 31, 2006

## Issue of File Transfer Impossibility in XFIT/S

### ■ Affected products

Corrective action	Product name	Platform	Last update
<a href="#">HS06-004-01</a>	XFIT/S, XFIT/S/JCA, XFIT/S/ZGN, XFIT/S ZENGIN TCP/IP Procedure	AIX, HI-UX/WE2	March 31, 2006

### ■ Problem description

When the above products receive data unexpectedly, the server process and the transfer control process of the above products sometimes stop, or transfer requests to the above products is sometimes not accepted.

When such a problem occurs, file transfer can become impossible.

### Revision history

- March 31, 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.

# 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](#) > 
 HS06-004-01

> 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



Update: March 31, 2006

### HS06-004; Issue of File Transfer Impossibility in XFIT/S

## Solutions for XFIT/S

When the port that XFIT/S provides receives data unexpectedly, the following problem sometimes occurs:

- When the platform is AIX, the server process and the transfer control process of XFIT/S sometimes stop, and then file transfer can become impossible.
- When the platform is HI-UX/WE2, transfer requests to XFIT/S are sometimes not accepted, and then file transfer can become impossible.

Fixed versions for the recent versions are available indicated below. Upgrade the XFIT/S version in your system to the appropriate version.

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

Product name	Model	Version	Platform	Fixed version	Release time	Last update
XFIT/S	P-1M41-911	01-00 to 01-00-/A	AIX	01-00-/B	September 9, 2004	March 31, 2006
XFIT/S/JCA	P-F1M41-9111	01-00 to 01-00-/A		01-00-/B	January 5, 2006	March 31, 2006
XFIT/S/ZGN	P-F1M41-9112	01-00 to 01-00-/B		01-00-/C	January 5, 2006	March 31, 2006
XFIT/S ZENGIN TCP/IP Procedure	P-F1M41-911A	01-00 to 01-00-/D		01-00-/E	January 5, 2006	March 31, 2006
XFIT/S	P-1641-911	01-08 to 01-13-/I	HI-UX/WE2	01-13-/J	March 6, 2006	March 31, 2006
XFIT/S/JCA	P-F1641-9111	01-03 to 01-05-/E		01-05-/F	March 6, 2006	March 31, 2006
XFIT/S/ZGN	P-F1641-9112	01-02-/F to 01-04-/D		01-04-/E	March 6, 2006	March 31, 2006
XFIT/S ZENGIN TCP/IP Procedure	P-F1641-911A	01-00 to 01-02-/C		01-02-/D	March 6, 2006	March 31, 2006

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

## [Workarounds]

Until the fixed modules are applied, carry out the following workarounds:

- Set filtering rules on the OS or router so that only reliable hosts can access the port that XFIT/S provides.

## Revision history

- March 31, 2006: Information about issue of file transfer impossibility in XFIT/S 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](#)