

Software Vulnerability Information

Software Division



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

[Japanese](#)

Search in the Hitachi site by Google



[Advanced search](#)

[Home](#) > [Vulnerability Information](#) > [Software Vulnerability Information](#) > HS05-011

Update: April 12, 2007

Vulnerability to miscontrol of PCMCIA devices by JP1/HIBUN

- Affected products

Corrective action	Product name	Platform	Last update
HS05-011-01	JP1/HIBUN Advanced Edition Information Cypher JP1/HIBUN Advanced Edition Information Fortress HIBUN Advanced Edition Information Cypher HIBUN Advanced Edition Information Fortress	Windows	April 12, 2007

- Problem description

A vulnerability was found for a hard disk connected to a PC based on the PCMCIA standard, with JP1/HIBUN incorrectly recognizing such a disk as an internal hard disk on Windows 2000 and Windows XP. As a result, there is a possibility that JP1/HIBUN cannot correctly control data taken out through the hard disk.

Please note JP1/HIBUN products are for Japanese systems only. JP1 is an abbreviation for Job Management Partner 1.

Revision history

- April 12, 2007: Corrective actions page is updated.
- March 10, 2006: Corrective actions page is updated.
- June 30, 2005: This page is released.

[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](#)

Software Vulnerability Information

Software Division



Update: April 12, 2007

HS05-011;
Vulnerability to miscontrol of PCMCIA devices by JP1/HIBUN

Solution for JP1/HIBUN

A vulnerability was found for a hard disk connected to a PC based on the PCMCIA standard, with JP1/HIBUN incorrectly recognizing such a disk as an internal hard disk. As result, there is a possibility that JP1/HIBUN cannot correctly control data taken out through the hard disk.

Fixed versions are available for the versions indicated below. Please upgrade the HIBUN version in your system to the appropriate version.

[Affected Products]

- Affected platforms
 - Windows 2000
 - Windows XP
- Affected PCMCIA devices
 - A PCMCIA hard disk that is separated into several partitions
 - An external hard disk that is connected with the PC based on PCMCIA standard

[Affected models, versions and fixed versions]

Product name	Model	Version	Platform	Fixed version (*1)	Release date	Last update
JP1/HIBUN Advanced Edition Server (*2)	R-1543H-11	07-00 - 07-00-/C			(*4)	April 12, 2007
		07-01 - 07-01-/B		07-01-/G	July 8, 2005	March 10, 2006
		07-10 - 07-10-/C		07-10-/E	July 5, 2005	March 10, 2006
		07-50 - 07-50-/B		07-50-/C	June 22, 2005	June 30, 2005

> 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



JP1/HIBUN Advanced Edition Information Cypher	R-1543H-71	07-00 - 07-00-/C	Windows	(*4)	April 12, 2007	
		07-01 - 07-01-/B		07-01-/G	July 8, 2005	March 10, 2006
		07-10 - 07-10-/C		07-10-/E	July 5, 2005	March 10, 2006
		07-50 - 07-50-/B		07-50-/C	June 22, 2005	June 30, 2005
HIBUN Advanced Edition Server (*3)	R-1V13-06W001F1	06-02		(*4)	April 12, 2007	
		06-03-/A		(*4)	April 12, 2007	
		06-04 - 06-04-/A		(*4)	April 12, 2007	
		06-05 - 06-05-/E		(*4)	April 12, 2007	
HIBUN Advanced Edition Information Cypher	R-1V13-07W001F1, R-1V13-07W001L1, R-1V13-07W001L2, R-1V13-07W001L3, R-1V13-07W001L4, R-1V13-07W001L5, R-1V13-07W001L8, R-1V13-07W001L9	06-02		(*4)	April 12, 2007	
		06-03-/A		(*4)	April 12, 2007	
		06-04 - 06-04-/A		(*4)	April 12, 2007	
		06-05 - 06-05-/E		(*4)	April 12, 2007	

(*1) If you use the server function, please apply the fixed version to the server first, and then the client.

(*2) If you use JP1/HIBUN Advanced Edition Information Fortress, you need to arrange the licenses of both JP1/HIBUN Advanced Edition Server and JP1/HIBUN Advanced Edition Information Fortress.

(*3) If you use HIBUN Advanced Edition Information Fortress, you need to arrange the licenses of both HIBUN Advanced Edition Server and HIBUN Advanced Edition Information Fortress.

(*4) Please upgrade the product to a newer version or revision. Alternatively, contact your Hitachi support service representative.

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

Revision history

- April 12, 2007: Information about fixed versions of all models is updated.
- March 10, 2006: Information about fixed versions of R-1543H-11 and R-1543H-71 is updated.
- June 30, 2005: Information about the vulnerability to miscontrol of PCMCIA devices by JP1/HIBUN 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](#)