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

HIRT Hitachi Incident Response Team

Update: April 12, 2007

Vulnerability to user privilege violations when using the view function in JP1/HIBUN

- Affected products

Corrective action	Product name	Platform	Last update
HS05-010-01	JP1/HIBUN Advanced Edition Information Cypher JP1/HIBUN Advanced Edition Information Fortress HIBUN Advanced Edition Information Cypher HIBUN Advanced Edition Information Fortress HIBUN/Enterprise Client HIBUN/Enterprise Client Extension Pack	Windows	April 12, 2007

- Problem description

A vulnerability was found in the above products where normal users can operate beyond their privileges when using the view function of HIBUN (HIBUN Viewer) from a client PC.
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.

- 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

Update: April 12, 2007

HS05-010;
Vulnerability to user privilege violations when using the view function in JP1/HIBUN

Solution for JP1/HIBUN

A vulnerability was found where normal users can operate beyond their privileges when using the view function of HIBUN (HIBUN Viewer) from a client PC. Fixed versions are available for the versions indicated below. Please upgrade the HIBUN version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version (*1)(*2)	Release date	Last update
JP1/HIBUN Advanced Edition Server (*3)	R-1543H-11	07-00 - 07-00-/C	Windows	(*6)		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
JP1/HIBUN Advanced Edition Information Cypher	R-1543H-71	07-00 - 07-00-/C		(*6)		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 (*4)	R-1V13-06W001F1	06-05 - 06-05-/E		(*6)		April 12, 2007

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

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	06-05 - 06-05-/E		(*6)	April 12, 2007
HIBUN/Enterprise Client (*5)	R-1V13-04W002L1, R-1V13-04W002L2, R-1V13-04W002L3, R-1V13-04W002L4, R-1V13-04W002L5, R-1V13-04W002L6, R-1V13-04W002L7, R-1V13-04W002L8	05-00 - 05-00-/B		(*6)	April 12, 2007
		05-01		(*6)	April 12, 2007
		05-02 - 05-02-/B		(*6)	April 12, 2007

(*1) Please apply the fixed version to the server first, and then the client.

(*2) The fixed version contains a few functional enhancements of HIBUN Viewer. For details about the enhancements, refer to the applicable documents for each product (such as software attachments).

(*3) 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.

(*4) 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.

(*5) HIBUN/Enterprise Client Extension Pack is also affected.

(*6) 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 user privilege violations when using the view function in JP1/HIBUN is released.

- 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