Search in the Hitachi site by Google
GO
> Advanced search

TOP

What's New

Notifications

Alert

Software Vulnerability Information

Links to Security Organizations

Update: November 18, 2005

DoS Vulnerability in Groupmax Web Workflow Server Set for Active Server Pages

- Affected products

Corrective action	Product name	Platform	Last update
HS05-012-01	Groupmax Web Workflow Server Set for Active Server Pages, Groupmax Form Version3 for Active Server Pages	Windows	November 18, 2005

- Problem description

A vulnerability to DoS (Denial of Service) attacks was found in the above products. The vulnerability can be exploited by malicious users inputting information, which includes a device name, that causes requests to be repeatedly sent to the server machine. Such repeated requests cause DoS, in which requests cannot be accepted until the server machine is rebooted.

Revision history

- November 18, 2005: Corrective actions page is updated.
- July 20, 2005: This page is released.

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

- 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

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: November 18, 2005

HS05-012;
DoS vulnerability in Groupmax Web Workflow Server Set for Active Server Pages

Solution for Groupmax Web Workflow Server Set for Active Server Pages

When performing operations on attached files of Groupmax Web Workflow Server Set for Active Server Pages or Groupmax Form Version3 for Active Server Pages, the vulnerability can be exploited by malicious users inputting information, which includes a device name, that causes requests to be repeatedly sent to the server machine. Such repeated requests cause DoS, in which requests cannot be accepted until the server machine is rebooted.
Fixed versions for the recent versions are available indicated below. Please upgrade the Groupmax version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release date	Last update
Groupmax Form Version3 for Active Server Pages	P-2446-7724	03-10 - 03-10-/D	Windows	06-52-/D (*1)	June 27, 2005	July 20, 2005
Groupmax Web Workflow Server Set for Active Server Pages	P-2446-7K34	05-00 - 05-00-/B, 05-10 - 05-10-/A, 05-11 - 05-11-/E, 05-20 - 05-20-/D		05-20-/E (*2)	October 28, 2005	November 18, 2005
	P-2446-7K44	06-00, 06-01 - 06-01-/A, 06-02, 06-03 - 06-03-/A, 06-50, 06-51 - 06-51-/A, 06-52 - 06-52-/C		06-52-/D (*2)	June 27, 2005	July 20, 2005

(*1) Please upgrade the version to model P-2446-7K44 version 06-52-/D or later.
(*2) Please upgrade the version to a fixed revision.

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

Revision history

- November 18, 2005: Information about fixed version of P-2446-7K34 is updated.

- July 20, 2005: Information about the DoS vulnerability in Groupmax Web Workflow Server Set for Active Server Pages 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