Software Vulnerability Information
Software Division

Update: October 29, 2004

DoS Vulnerability in Web Page Generator

- Affected product

Corrective actions	Product name	Platform	Last update
HS04-002-01	Web Page Generator	Windows	October 29, 2004

- Problem description

  If a website using the above product is improperly accessed, a response may not be returned to the web browser. Moreover, if the invalid access is repeated, the website functionality may stop.

Revision history

- October 29, 2004: Corrective actions page is updated.
- August 6, 2004: Corrective actions page is updated.
- July 28, 2004: 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.

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.

HIRT Hitachi Incident Response Team

Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

Software Vulnerability Information
Software Division

HITACHI
Inspire the Next

| Home | Software | ≫ Security |

Update: October 29, 2004

HS04-002;
DoS Vulnerability in Web Page Generator

Solution for Web Page Generator

If a website using the above product is improperly accessed, a response may not be returned to the web browser. Moreover, if the improper access is repeated, the website functionality may stop.
Fixed versions are available for the newest version of each model. Please apply the fixed version to your system.
As for the corrected versions, contact your Hitachi support service representative.

[Affected models, versions and fixed versions]

Model	Product name	Version	Platform	Fixed version	Release time	Last update
P-F2463-61141	Web Page Generator	01-00 - 01-01-/C	Windows	(*1)		July 28, 2004
P-2451-2124	Web Page Generator	02-00 - 02-00-/C		(*1)		July 28, 2004
P-2451-2134	Web Page Generator Enterprise 3.0	03-00 - 03-02-/C		03-03-/D (*2)	July 15, 2004	October 29, 2004
		03-03 - 03-03-/C		03-03-/D	July 15, 2004	July 28, 2004
P-2451-2154	Web Page Generator Enterprise 4.0	04-00 - 04-00-/C		04-02-/L (*2)	July 15, 2004	October 29, 2004
		04-02 - 04-02-/K		04-02-/L	July 15, 2004	July 28, 2004

(*1) Please upgrade the version to 03-03-/D of model P-2451-2134 or 04-02-/L of model P-2451-2154.
(*2) Please upgrade the version to a fixed version.

[Workaround]

> 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

The following workaround may be applied to circumvent this vulnerability. Please apply the workaround until the fixed version is applied to your system.

- Model: P-F2463-61141, P-2451-2124, P-2451-2134

  No workaround exits.

- Model: P-2451-2154

1. When "2" is specified for the PAGE_GENERATOR_EDITION property in the runtime environment definition file (WebPGen.cfg):

   Application of the template file analysis engine intermediate language generation mode is specified. This problem will not occur in this case.

2. When "2" is not specified for the PAGE_GENERATOR_EDITION property in the runtime environment definition file (WebPGen.cfg): (No specification is made or the specification has been changed to normal mode)

   (1) Setting in the configuration file
        By setting the following definitions in the runtime environment definition file (WebPGen.cfg), the template file analysis engine of the intermediate language generation mode will be used. In addition, this problem will not occur in intermediate language generation mode.

        Definition example

        ```
        PAGE_GENERATOR_EDITION= 2
        ```

   (2) Change necessary in the system
        When the above setup is completed, the template file will be interpreted and executed in the intermediate language generation mode. In this case, the following change is needed.

        (a) It is necessary to specify the compatible option with the normal mode in the runtime environment definition file (WebPGen.cfg). (For details, see the README.)
        (b) In the intermediate language generation mode, since the comment format of the macro definition file (Macro.cfg) and the method definition file (Method.cfg) are changed to "<!@BCOMMENT>~ <!/BCOMMENT>" from "#", the items such as the macros and methods are commented out by "#" and loaded. Therefore, it is necessary to change the macro definition file and the method definition file.
        (c) In the intermediate language generation mode, since the template file analysis is strictly processed and syntax errors may occur, there are cases in which a template file must be corrected. (For details, see the manual.)
        (d) In the intermediate language generation mode, more memory and disk space are required compared with the normal mode for the cache function of intermediate language generation. Therefore, it is

necessary to estimate this capacity beforehand. (For details, refer to the README.)

Revision history

- October 29, 2004: Information about fixed versions of P-2451-2134 and P-2451-2154 is updated.
- August 6, 2004: The information about obtaining the corrected versions is added.
- July 28, 2004: 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.

 Page Top