

# Software Vulnerability Information

## Software Division



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

» [Japanese](#)

Search in the Hitachi site by Google



> [Advanced search](#)

[Home](#) > [Vulnerability Information](#) > [Software Vulnerability Information](#) > [HS04-003](#)

Update: July 28, 2004

## Vulnerability Issue in Error Transactions of Web Page Generator Templates

- Affected product

Corrective actions	Product name	Platform	Last update
<a href="#">HS04-003-01</a>	Web Page Generator	Windows, HP-UX 11.0, AIX5.1, Solaris	July 28, 2004

- Problem description

The following problems may occur, when the above products are used in debugging mode (DEBUG\_MODE=on), and when the default error template is used:

- Information about an internal directory is displayed.
- A crossing-site scripting problem is generated.

### Revision history

- 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

> [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](#)



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



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

[» Japanese](#)

Search in the Hitachi site by Google



[» Advanced search](#)

[Home](#) > [Vulnerability Information](#) > [Software Vulnerability Information](#) > [HS04-003-01](#)

Update: July 28, 2004

### HS04-003; Vulnerability Issue in Error Transactions of Web Page Generator Templates

## Solution for Web Page Generator

A vulnerability issue in error transactions of the Web Page Generator templates was found. The workaround for this problem is as follows:

#### [Affected models and versions]

Model	Product name	Version	Platform
P-F2463-61141	Web Page Generator	01-00 - 01-01-/C	Windows
P-2451-2124	Web Page Generator	02-00 - 02-00-/C	
P-2451-2134	Web Page Generator Enterprise 3.0	03-00 - 03-03-/D	
P-2451-2154	Web Page Generator Enterprise 4.0	04-00 - 04-02-/L	
P-1B51-9121	Web Page Generator	02-00 - 02-00-/C	HP-UX 11.0
P-1B51-9331	Web Page Generator Enterprise 3.0	03-00 - 03-03-/C	
P-1B51-9351	Web Page Generator Enterprise 4.0	04-01 - 04-07-/A	
P-1M51-9141	Web Page Generator Enterprise 4.0	04-05 - 04-06-/C	AIX 5.1
P-9D51-9151	Web Page Generator Enterprise 4.0	04-01 - 04-01-/B	Solaris

#### [Workaround]

- Setting in the configuration file  
Set "off" for the DEBUG\_MODE property of the runtime environment definition file (WebPGen.cfg), and use the error template.  
(To have error processing perform when DEBUG\_MODE=on and an error message is embedded in an HTML document, it is necessary to use an error template.)

```
DEBUG_MODE=off
```

- Required modifications of the error template  
The error template must be changed so that another message about an error message including file information may be displayed.  
To prevent the script embedded in the error message from being executed, the escape process must be performed in a string of the error message.

[» 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](#)



## <Example>

The following is an example of changing the error template.

- File information must be removed out of the message when the template file fails to open (error code : 1040).  
The display of "failure of opening of the template file (c:¥xxx ¥yyy.pgt)" must be changed to "failure of opening of the template file."
- When displaying the error message (\$ERROR\_MESSAGE variable), escape processing must be performed using the ESCAPE extension tag in a variable.

```
<html>
<body>
<hr>
Template used when an error occurs
<hr>
<br>
ERROR_CODE = $ERROR_CODE<br>
<!--@IF CND = ($ERROR_CODE == 1040)>
  failure of opening of the template file<br>
<!--@ELSE>
  ERROR_MESSAGE <##ESCAPE($ERROR_MESSAGE) ><br>
<!--/IF>
</body>
</html>
```

For details about the error messages that output file information, see the error message tables in the appendix of the Web Page Generator Enterprise User's Guide.

## Revision history

- 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](#)