Update: September 8, 2003

Vulnerability Related to Hijacking of Web Application Sessions Through the Malicious Monitoring of Cookies

- Affected product

Corrective actions	Product name	Platform	Last update
HS03-005-01	Web Page Generator Enterprise	Windows NT/2000, HP-UX 11.0/11i, AIX 5.1, Solaris 2.6/7	September 8, 2003

We are currently examining the effect on products other than those listed above.

- Problem description

  The technical report (AIST03-J00017(Japanese)) issued by the Grid Technology Research Center of the National Institute of Advanced Industrial Science and Technology on July 17, 2003 identified a problem related to session hijacking.
  The problem is that information may be leaked as the result of impersonation following the malicious monitoring of cookies and other such acts when the user is using cookies in non-secure mode.

Revision history

- September 8, 2003: 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

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

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: September 8, 2003

HS03-005;
Vulnerability Related to Hijacking of Web Application Sessions Through Malicious Monitoring of Cookies

Workaround for Web Page Generator Enterprise

A vulnerability related to hijacking of Web application sessions through malicious monitoring cookies has been found in Web Page Generator Enterprise.
This problem occurs when the `Secure` attribute is not set for cookies that manage a session. The following explains how to avoid this problem.

[Workaround]

(1) Setting in the configuration file

You can set the `Secure` attribute for cookies that manage a Web Page Generator session by defining the value shown below in the configuration file (`WebPGen.cfg`) of Web Page Generator.

Example definition:

```
COOKIE_PATH=/; Secure
```

(2) Required system modifications

After you have set the above value, cookies pass along the communication channel only when you access a URL starting with `https://`. You must therefore set HTTPS (SSL connection) for all access to pages that use Web Page Generator. Therefore:

(a) When HTTPS is set for all current sites:

You can avoid the problem simply by setting the value given in (1) above.

(b) When HTTP and HTTPS are set for different sites:

You must either set HTTPS for all sites or set HTTPS only for pages that must inherit a session.

[Note]

- You can apply the above method only on version 03-02 or later. If you are using 03-01 or an earlier version, replace it with Windows version 03-03 or HP-UX version 03-02 and then apply the above-mentioned method for avoiding the problem.

[Affected versions]

Model	Version	Platform
P-F2463-61141	01-00 - 01-01-/C	Windows NT
P-2451-2124	02-00 - 02-00-/C	Windows NT
P-2451-2134	03-00 - 03-03-/B	Windows NT, Windows 2000
P-2451-2154	04-00 - 04-02-/I	Windows NT, Windows 2000
P-1B51-9121	02-00 - 02-00-/C	HP-UX 11.0
P-1B51-9331	03-00 - 03-03-/C	HP-UX 11.0, 11i
P-1B51-9351	04-01 - 04-07-/A	HP-UX 11.0, 11i
P-1M51-9141	04-05 - 04-06	AIX 5.1
P-9D51-9151	04-01 - 04-01-/B	Solaris 2.6, 7

Revision history

- September 8, 2003: 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