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: July 14, 2003

Cross-site Scripting Vulnerability on Apache HTTP Server

On October 2, 2002, an advisory on a cross-site scripting vulnerability on Apache HTTP Server from Apache Software Foundation (Bugtraq-id: 5847) has been released. This cross-site scripting vulnerability affects Hitachi Web Server as well, since it employs Apache HTTP Server. Take the following countermeasures to handle this problem.

■ Affected Products

The following table lists the products that have this vulnerability.

No.	Model	Product name	Version	Platform
1	P-1B41-E111	Hitachi Web Server	01-00 - 01-00/B, 01-01 - 01-01/B, 01-02 - 01-02/C	HP-UX10.20
2	P-1B41-E121	Hitachi Web Server	01-00 - 01-00/B, 01-01 - 01-01/B, 01-02 - 01-02/C	HP-UX11.0/11i
3	P-1B41-E121B1	Hitachi Web Server	01-00 - 01-00/A, 01-01 - 01-01/A, 01-02 - 01-02/C	HP-UX11.0/11i
4	P-1M41-E111	Hitachi Web Server	01-01 - 01-01/B, 01-02 - 01-02/C	AIX5L V5.1
5	P-1L41-E111	Hitachi Web Server	01-01	Turbolinux Server 6 for MP Series
			01-01-A	Turbolinux Server 7 for AP8000
6	P-2441-E151	Hitachi Web Server	02-00	Windows NT 4.0 Workstation/Server, Windows 2000

				Server/ Advanced Server/ Datacenter Server
7	P-9D41-E111	Hitachi Web Server	01-00 - 01-00/B, 01-01 - 01-01/B, 01-02 - 01-02/C	Solaris2.6/7/8/9
8	P-9S41-E111	Hitachi Web Server	01-01 - 01-01/B	Turbo Linux Japanese version 6.1, RedHat Linux 6.2 Japanese version

■Detail of the problem

Hitachi Web Server omits some escape processes (such as converting "<" to "<"), which should be intrinsic specifications, when outputting error screens under certain conditions. This may allow for illegal script executions. A malicious third party might exploit this and cause the cross-site scripting problem.

■Conditions

When `Off` is specified for the `UseCanonicalName` directive (the `UseCanonicalName` directive is `On` by default), and its Web server host name is specified as a wild card on the DNS (Domain Name System) server.

■Countermeasures

Make one of the following modifications.

- Specify `On` for the `UseCanonicalName` directive.
- Avoid using a wild card specification (specify a host name at a time).
- Customize the configuration using the `ErrorDocument` directive.
  For details on the `ErrorDocument` directive, see the manual "*Hitachi Web Server*".

Revision history

- July 14, 2003: This page is released.

---

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