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: August 5, 2003

Vulnerability Related to Apache HTTP Server

- Affected products

Corrective actions	Product name	Platform	Last update
HS03-003-01	Hitachi Web Server	Windows	August 5, 2003

- Problem description

  On July 21, 2003, CERT/CC released a vulnerability problem on URI requests regarding Apache HTTP Server (VU#694428).
  This problem occurs in Apache HTTP Server running on the Win32 system, which is configured to use rotatelogs. If a crafted URI Request is issued on Apache HTTP Server having such a configuration, log collection is forcibly terminated.

Revision history

- August 5, 2003: This page is released.

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: August 5, 2003

HS03-003;
Vulnerability Related to Apache HTTP Server

Modification in Hitachi Web Server

A vulnerability in the rotatelogs utility of Hitachi Web Server was identified. Hitachi provides the appropriate patch. Please apply it to your system.

Contact your Hitachi support service representative for the patch.

[Note]

- If the patch cannot be applied, avoid this vulnerability by using a system configuration that enables access log and error log collection without the rotatelogs utility. Log files are increased monotonously in this case, so they should be saved and deleted periodically.

Model	Version	Platform
P-2441-E151	02-00 - 02-00-/B, 02-01	Windows 2000, Windows NT

Apply the patch to Hitachi Web Server included in the following Cosminexus Server products as well:

Cosminexus product	Model	Version	Platform
Cosminexus Application Server Version 5	P-2443-1D54	05-01 - 05-01-/C, 05-05	Windows 2000, Windows NT
Cosminexus Developer Version 5	P-2443-1F54	05-01 - 05-01-/C, 05-05	Windows 2000, Windows NT

Revision history

- August 5, 2003: The patch for the vulnerability in versions 02-00 and 02-01 is now available.

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