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

Vulnerability Related to Apache Web Server

On June 17, 2002, the CERT/CC released an advisory about a security problem related to Apache Web servers (Advisory CA-2002-17)
This advisory reported that a remotely exploitable vulnerability was found in the way that Apache web servers handled chunk-encoded data. *This vulnerability may enable remote attackers to execute their own commands and perform denial-of-service (DoS) attacks.*

This problem affects the following product from Hitachi Software Division. We will provide information about this product, including the procedure for solving the problem.

■ Affected product (Last update: July 14, 2003)

Corrective actions	Product name	Platform	Last update
HS02-008-01	JP1/Cm2/Network Node Manager	HP-UX, Solaris	July 14, 2003
HS02-008-02	Hitachi Web Server	HP-UX,Solaris,AIX,Linux	July 14, 2003

❖ In this homepage, Job Management Partner 1/Consolidated Management 2 is abbreviated as JP1/Cm2.

Revision history

- July 14, 2003: This page is revamped.

---

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: July 14, 2003

HS02-008;
Vulnerability Related to Apache Web Server

Modification in JP1/Cm2/Network Node Manager

The Computer Emergency Response Team Coordination Center (CERT/CC) that researches and reports on Internet security released the advisory titled *Apache Web Server Chunk Handling Vulnerability*. This advisory reported that Apache web servers contain a remotely exploitable vulnerability in handling chunk-encoded data. For details, see Advisory CA-2002-17.

The Web server of JP1/Cm2/Network Node Manager also contains this vulnerability.

1. Phenomenon
The Web server process of JP1/Cm2/Network Node Manager may terminate abnormally with a segmentation fault if the server process receives an invalid chunk-encoded request. If the Web server process terminates abnormally, the control process starts another server. This creates the load of outputting a core dump and restarting the server process. Invalid requests that a malicious party sends in succession may lead to a denial of service (DoS) attack.

2. Affected models and versions, and patches
The following patches are now available for the affected platforms and versions.

3. Other information
Other versions are under investigation.

Models and versions of JP1/Cm2/Network Node Manager affected by the vulnerability

- **Japanese version**

Model	Version	Platform	Patch		Fixed version	Last update
			Application procedure	Download		
P-1B42-6161 P-1B42-6261	06-71	HP-UX	HS02-008-01-a	P-1B42-6161_0671SA.tar (890,880byte)	06-71-/A	July 14, 2003
P-9D42-6161	06-71	Solaris	HS02-008-01-b	P-9D42-6161_0671SA.tar (587,776byte)	06-71-/A	July 14,

P-9D42-6261						2003
P-1B42-6161 P-1B42-6261	06-51	HP-UX	HS02-008-01-c	P-1B42-6161_0651SC.tar (890,880byte)	06-51-/A	July 14, 2003
P-9D42-6161 P-9D42-6261	06-51	Solaris	HS02-008-01-d	P-9D42-6161_0651SC.tar (587,776byte)	06-51-/A	July 14, 2003
P-1B42-6161 P-1B42-6261	06-50 - 06-50-/A	HP-UX	HS02-008-01-e	P-1B42-6161_0650SK.tar (890,880byte)	06-50-/B	July 14, 2003
P-9D42-6161 P-9D42-6261	06-50 - 06-50-/A	Solaris	HS02-008-01-f	P-9D42-6161_0650SB.tar (587,776byte)	06-50-/B	July 14, 2003
P-1B42-6161 P-1B42-6261	06-00 - 06-00-/A	HP-UX	HS02-008-01-g	P-1B42-6161_0600SF.tar (890,880byte)	06-00-/B	July 14, 2003
P-9D42-6161 P-9D42-6261	06-00 - 06-00-/C	Solaris	HS02-008-01-h	P-9D42-6161_0600SC.tar (587,776byte)	06-00-/D	July 14, 2003

❖ There are no prerequisite patches related to these patches.

Revision history

- July 14, 2003: This page is revamped.
- October 11, 2002: Security patches for version 06-00 and 06-50 are released.

Page Top

| Term of Use | Privacy Notice | About Hitachi |

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

HS02-008;
Vulnerability Related to Apache Web Server

Modification in Hitachi Web Server

The Computer Emergency Response Team Coordination Center (CERT/CC) that researches and reports on Internet security released the advisory titled *Apache Web Server Chunk Handling Vulnerability*. This advisory reports the problem that the chunk format data processing on Apache Web Server has a vulnerability to unauthorized remote access. For details, see Advisory CA-2002-17.

Hitachi Web Server also has the same vulnerability.

1. Phenomenon
When Hitachi Web Server has received invalid requests in the chunk format, Hitachi Web Server's server processes may terminate abnormally due to a segmentation fault. When server processes have terminated abnormally, the control process starts new server processes, but this results in increased loads for core dump output and server process restart. A malicious third party might exploit this problem and launch a DoS (Denial of Service) attack by continuously sending such invalid requests.

2. Applicable models or versions, and distribution of fixing patches
Contact your Hitachi support service representative.

Models and versions of Hitachi Web Server affected by the vulnerability

Product name	Model	Ver-Rev	Platform
Hitachi Web Server	P-1B41-E111	01-02-/A 01-02 01-01-/A 01-01 01-00-/A 01-00	HP-UX10.20
	P-1B41-E121 P-1B41-E121B1	01-02-/A 01-02 01-01-/A 01-01 01-00-/A 01-00	HP-UX11.0/11i

	P-1M41-E111	01-02 01-01	AIX5L V5.1
	P-1L41-E111	01-01	Turbolinux Server 6 for MP Series
	P-9D41-E111	01-02 01-01 01-00-/A 01-00	Solaris2.6/7/8
	P-9S41-E111	01-01-/A 01-01	Turbo Linux Japanese verion 6.1, RedHat Linux 6.2 Japanese version

This vulnerability problem affects Hitachi Web Server included in the following Cosminexus Server products as well.

Cosminexus product	Model	Platform
Cosminexus Server - Web Edition	P-1BZ4-1S31	HP-UX11.0/11i
	P-9DZ4-1D31	Solaris2.6/7
Cosminexus Server - Standard Edition	P-1BZ4-1T31	HP-UX11.0/11i
	P-9DZ4-1E31	Solaris2.6/7
Cosminexus Server - Enterprise Edition	P-1BZ4-1U31	HP-UX11.0/11i
	P-9DZ4-1F31	Solaris2.6/7
Cosminexus Server - Web Edition Version 4	P-1BZ4-1S41	HP-UX11.0/11i
	P-9DZ4-1D41	Solaris7/8
Cosminexus Server - Standard Edition Version 4	P-1BZ4-1T41	HP-UX11.0/11i
	P-9DZ4-1E41	Solaris7/8
	P-1MZ4-1E41	AIX5L V5.1

Revision history

- July 14, 2003: This page is revamped.

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

Page Top