Update: May 23, 2005

DoS Vulnerability in JP1/Cm2/Network Node Manager

- Affected products

Corrective action	Product name	Platform	Last update
HS05-008-01	JP1/Cm2/Network Node Manager Enterprise, JP1/Cm2/Network Node Manager 250, JP1/Cm2/Network Node Manager	HP-UX, Windows, Solaris	May 23, 2005

- Problem description

Vulnerability to DoS (Denial of Service) attacks was found in the above products. Malicious users can exploit the vulnerability and cause DoS in the above products.

Revision history

- May 23, 2005: 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.

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

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: May 23, 2005

HS05-008;
DoS Vulnerability in JP1/Cm2/Network Node Manager

Solution for JP1/Cm2/Network Node Manager

The following vulnerability was found in JP1/Cm2/Network Node Manager (NNM):
If a malicious user sends invalid data to a port that an NNM process is using, the process using that port will end abnormally, or the CPU will be completely occupied resulting in DoS (denial of service) for NNM. If DoS for NNM occurs, the NNM service must be restarted.
Fixed versions are available for the versions indicated below. Please upgrade the NNM version in your system to the appropriate version.

[Influence]

This vulnerability does not affect NNM version 07-10, however, it affects versions that are older than those listed in the table below, so please upgrade the appropriate products or carry out the workarounds.

[Affected models and versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
JP1/Cm2/Network Node Manager Enterprise	P-1B42-6161	06-00 - 06-51-/A	HP-UX	06-71-/C (*1)	December 3, 2004	May 23, 2005
		06-71 - 06-71-/B		06-71-/C	December 3, 2004	May 23, 2005
	P-2442-6164	06-00 - 06-51-/B	Windows	06-71-/C (*1)	December 3, 2004	May 23, 2005
		06-71 - 06-71-/B		06-71-/C	December 3, 2004	May 23, 2005
	P-9D42-6161	06-00 - 06-51-/B	Solaris	06-71-/C (*1)	December 3, 2004	May 23, 2005
		06-71 - 06-71-/B		06-71-/C	December 3, 2004	May 23, 2005

JP1/Cm2/Network Node Manager 250	P-1B42-6261	06-00 - 06-51-/A	HP-UX	06-71-/C (*1)	December 3, 2004	May 23, 2005
		06-71 - 06-71-/B		06-71-/C	December 3, 2004	May 23, 2005
	P-2442-6264	06-00 - 06-51-/B	Windows	06-71-/C (*1)	December 3, 2004	May 23, 2005
		06-71 - 06-71-/B		06-71-/C	December 3, 2004	May 23, 2005
	P-9D42-6261	06-00 - 06-51-/B	Solaris	06-71-/C (*1)	December 3, 2004	May 23, 2005
		06-71 - 06-71-/B		06-71-/C	December 3, 2004	May 23, 2005
JP1/Cm2/Network Node Manager	P-1B42-6271	07-00 - 07-00-/A	HP-UX	07-01-/B (*1)	January 1, 2005	May 23, 2005
		07-01 - 07-01-/A		07-01-/B	January 1, 2005	May 23, 2005
	P-2442-6274	07-00 - 07-00-/A	Windows	07-01-/B (*1)	January 1, 2005	May 23, 2005
		07-01 - 07-01-/A		07-01-/B	January 1, 2005	May 23, 2005
	P-9D42-6271	07-00 - 07-00-/A	Solaris	07-01-/B (*1)	January 1, 2005	May 23, 2005
		07-01 - 07-01-/A		07-01-/B	January 1, 2005	May 23, 2005

(*1) Please upgrade the version to the fixed revision. To upgrade this NNM revision, some linked products that operate on NNM also need to be upgraded. For details about the appropriate versions for NNM and products linked to NNM, refer to the applicable documents for each product (such as software attachments or Readme).

For the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Before applying the fixed versions, carry out the following workarounds:
Set filtering for the firewall or router so the TCP port that NNM uses can only communicate with reliable parties.

Revision history

- May 23, 2005: Information about the DoS vulnerability in JP1/Cm2/Network Node Manager 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