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 20, 2006

Multiple Vulnerabilities of Web Utility Function of JP1/Cm2/Network Node Manager

- Affected products

Corrective action	Product name	Platform	Last update
HS05-018-01	Cm2/Network Node Manager Enterprise, Cm2/Network Node Manager Unlimited, Cm2/Network Node Manager 250, JP1/Cm2/Network Node Manager Enterprise, JP1/Cm2/Network Node Manager 250, JP1/Cm2/Network Node Manager	HP-UX, Windows, Solaris, HI-UX/WE2	July 20, 2006

- Problem description

Multiple vulnerabilities were found in the web utility function of the above products. Malicious users can exploit vulnerabilities, disable the services of JP1/Cm2/Network Node Manager, and execute arbitrary commands.

Revision history

- July 20, 2006: Corrective actions page is updated.
- November 18, 2005: Corrective actions page is updated.
- September 30, 2005: 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

| 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 20, 2006

HS05-018;
Multiple Vulnerabilities of Web Utility Function of JP1/Cm2/Network Node Manager

Solution for JP1/Cm2/Network Node Manager

Multiple vulnerabilities were found in the web utility function of JP1/Cm2/Network Node Manager (NNM). Malicious users can exploit these vulnerabilities and affect the system as explained below.

Vulnerability #1: DoS (Denial of Service) might occur for the web utility function of NNM due to unsuitable HTTP requests.
Vulnerability #2: Arbitrary commands might be executed due to unsuitable HTTP requests.
Vulnerability #3: The web authentication function might not be enabled.

Affected models and versions of NNM and the workarounds are indicated below. Carry out the workarounds or upgrade the NNM version in your system to the appropriate version.

[Affected models and versions]

Product name	Model	Version	Platform	Vulnerabilities(*1)		
				#1	#2	#3
Cm2/Network Node Manager Enterprise	P-1B42-5111	05-00 - 05-00-/C	HP-UX	Yes	No	No
	P-1642-511	05-00	HI-UX/WE2	Yes	No	No
Cm2/Network Node Manager Unlimited	P-2442-5194	05-00 - 05-00-/A	Windows	Yes	No	No
Cm2/Network Node Manager 250	P-1B42-5211	05-00 - 05-00-/C	HP-UX	Yes	No	No
	P-2442-5294	05-00 - 05-00-/A	Windows	Yes	No	No
	P-1642-521	05-00	HI-UX/WE2	Yes	No	No
	P-1B42-6111	05-20 - 05-20-/E	HP-UX	Yes	Yes	No
	P-1B42-6161	06-00 - 06-50-/A		Yes	Yes	No
		06-51 - 06-71-/C		Yes	Yes	Yes
	P-2442-	05-20 - 05-20-/F		Yes	Yes	No

JP1/Cm2/Network Node Manager Enterprise	6194		Windows			
	P-2442-6164	06-00 - 06-50-/A		Yes	Yes	No
		06-51 - 06-71-/D		Yes	Yes	Yes
	P-9D42-6111	05-20 - 05-20-/E	Solaris	Yes	Yes	No
	P-9D42-6161	06-00 - 06-50-/A		Yes	Yes	No
		06-51 - 06-71-/C		Yes	Yes	Yes
JP1/Cm2/Network Node Manager 250	P-1B42-6211	05-20 - 05-20-/E	HP-UX	Yes	Yes	No
	P-1B42-6261	06-00 - 06-50-/A		Yes	Yes	No
		06-51 - 06-71-/C		Yes	Yes	Yes
	P-2442-6294	05-20 - 05-20-/F	Windows	Yes	Yes	No
	P-2442-6264	06-00 - 06-50-/A		Yes	Yes	No
		06-51 - 06-71-/D		Yes	Yes	Yes
	P-9D42-6211	05-20 - 05-20-/E	Solaris	Yes	Yes	No
	P-9D42-6261	06-00 - 06-50-/A		Yes	Yes	No
		06-51 - 06-71-/C		Yes	Yes	Yes
JP1/Cm2/Network Node Manager	P-1B42-6271	07-00 - 07-10-02	HP-UX	Yes	Yes	Yes
		07-10-03		No	Yes	Yes
	P-2442-6274	07-00 - 07-10-02	Windows	Yes	Yes	Yes
		07-10-03		No	Yes	Yes
	P-9D42-6271	07-00 - 07-10-02	Solaris	Yes	Yes	Yes
		07-10-03		No	Yes	Yes

(*1) "Yes": The product contains the vulnerability for that column.
"No": The product does not contain the vulnerability for that column.

[Fixed versions]

Product name	Model	Version	Platform	Fixed version	Release date	Last update
JP1/Cm2/Network Node Manager Enterprise	P-1B42-6161	06-00 - 06-71-/C	HP-UX	(*4)		July 20, 2006
	P-2442-6164	06-00 - 06-71-/D	Windows	(*4)		July 20, 2006
	P-9D42-6161	06-00 - 06-71-/C	Solaris	(*4)		July 20, 2006
JP1/Cm2/Network Node Manager 250	P-1B42-6261	06-00 - 06-71-/C	HP-UX	(*4)		July 20, 2006
	P-2442-6264	06-00 - 06-71-/D	Windows	(*4)		July 20, 2006
	P-9D42-6261	06-00 - 06-71-/C	Solaris	(*4)		July 20, 2006
	P-1B42-	07-00 - 07-01-/B	HP-UX	07-10-04 (*2)	October 21, 2005	November 18, 2005

JP1/Cm2/Network Node Manager	6271	07-10 - 07-10-03		07-10-04 (*3)	October 21, 2005	November 18, 2005
	P-2442-6274	07-00 - 07-01-/B	Windows	07-10-04 (*2)	October 21, 2005	November 18, 2005
		07-10 - 07-10-03		07-10-04 (*3)	October 21, 2005	November 18, 2005
	P-9D42-6271	07-00 - 07-01-/B	Solaris	07-10-04 (*2)	October 21, 2005	November 18, 2005
		07-10 - 07-10-03		07-10-04 (*3)	October 21, 2005	November 18, 2005

(*2) Upgrade this version.
Note that products that operate while linked to NNM might also have to be upgraded. For the appropriate version of such linked products, refer to the applicable documentation for that product (such as readme files or documentation provided with the software).

(*3) NNM 07-10-02 or 07-10-03 is a prerequisite for the fixed version (accumulative patch) NNM 07-10-04. If your system uses NNM 07-10 or 07-10-01, an overwrite installation must be performed for NNM 07-10-02 before applying NNM 07-10-04.
Alternatively, if your system uses NNM 07-10-02 or 07-10-03 and workaround #2 (below) has been carried out, restore the CGI programs to their original directories before applying NNM 07-10-04.

(*4) For detailed information about this model, contact your Hitachi support service representative.

For the fixed versions and older versions not mentioned in the above table, contact your Hitachi support service representative.

[Workarounds]
Until the fixed versions are released, carry out both of the workarounds indicated below.

Workaround #1: (Workaround for vulnerability #1 and #3)
Set filtering for the firewall or router so that the TCP port that the web server for the web utility function of NNM uses can only communicate with reliable parties.

Workaround #2: (Workaround for vulnerability #2)
When the following version number of NNM matches your system, move the corresponding CGI programs that NNM supplies to any other new directory.

- connectedNodes.ovpl (In the case of NNM 06-51 or later)
- cdpView.ovpl (In the case of NNM 06-51 or later)
- freeIPaddrs.ovpl (In the case of NNM 06-51 or later)
- ecscmg.ovpl (*4) (In the case of NNM 05-20 or later)

(*4) This CGI program is being examined to determine whether it is vulnerable.

The above CGI programs are placed in the following path.

- Windows
  <*installation-folder-for-NNM*>\www\cgi-bin
- UNIX
  /opt/OV/www/cgi-bin

Performing the workarounds and moving the CGI programs affects NNM functions as follows.

- connectedNodes.ovpl
  The GUI menu for "Port/Address Mapping" becomes disabled.
- cdpView.ovpl
  The CDP view becomes disabled.
- freeIPaddrs.ovpl
  The GUI menu for "IP addresses not in use" becomes disabled.
- ecscmg.ovpl
  The configuration for actions triggered by events becomes disabled.

Revision history

- July 20, 2006: Information about fixed versions and release dates of P-1B42-6161, P-2442-6164, P-9D42-6161, P-1B42-6261, P-2442-6264, and P-9D42-6261 is updated.
- November 18, 2005: Information about vulnerabilities and fixed versions is updated.
- September 30, 2005: Information about the multiple vulnerabilities of web utility function of JP1/Cm2/Network Node Manager is released.

Page Top

| Term of Use | Privacy Notice | About Hitachi |