Update: July 14, 2003

Vulnerabilities Related to SNMP

On February 12, 2002, the CERT/CC released an advisory about security problems related to SNMP (Advisory CA-2002-03).

The Simple Network Management Protocol (SNMP) is a protocol that is widely used to manage network devices. This advisory reported that SNMP packets could not be processed properly in many implementations of the version 1 of this protocol. This may cause a problem in the network devices, Unix systems, Windows, and SNMP software that run on these operating systems. *This problem may cause a denial-of-service (DoS) attack, and enables an unauthorized party to obtain the administrator's privilege for the network device.*

This security problem affects the following products from Hitachi Software Division. This problem does not affect HI-UX/WE2 developed by Hitachi, because this operating system does not include the SNMP daemon (service).

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

Corrective actions	Product name	Platform	Last update
HS02-006-01	JP1/Cm2/Network Node Manager	HP-UX, Solaris, Windows	July 14, 2003
HS02-006-02	JP1/Cm2/Extensible Agent	Windows	July 14, 2003
HS02-006-03	JP1/Cm2/Extensible SNMP Agent	HP-UX, Solaris, AIX, Linux, Tru64, HI-UX/WE2	July 14, 2003
HS02-006-04	JP1/Cm2/SubManager	HP-UX, Solaris, AIX, HI-UX/WE2, Windows	July 14, 2003
HS02-006-05	JP1/Cm2/Hierarchical Agent	HP-UX, Solaris, Windows	July 14, 2003
HS02-006-06	Hitachi Directory Server Version 2	HP-UX	July 14, 2003

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

❖ We will provide patches for the above five products for each platform, as we complete each of them.

- Solaris, HP-UX, Windows, Linux, AIX

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

- Oracle DataBase
- UnixWare 7 Media Kit (CALDERA)
- iPlanet Directory Server, iPlanet Web Proxy Server
- IntranetWare, NetWare

  (The security patches are provided for the above products. For details, see Vendor's Web Sites.
  For AIX, IBM reported that a problem has been found. We have also included AIX in the affected products.)

- SCO UnixWare2.1J PE, SCO UnixWare2.1J AS

  (For SCO UnixWare, we will inform all our SCO UnixWare-using customers about how to address the problem.)

We recommend that you perform either of the following on your system until application of the patches to the above products is completed.

1. Stop unnecessary SNMP services (this disables system monitoring using SNMP).
2. Inhibit SNMP access from unauthorized hosts (for example, block the UDP port 161 or 162).
3. Reference the Web sites of vendors and apply the patches if they are provided.

[Vendor's Web Sites]

- Microsoft Corporation
- Hewlett-Packard Company
  Note: When you apply the HP-UX patches, click here to see the precautions.
- Sun Microsystems, Inc.
- Red Hat, Inc.
- TurboLinux Japan K.K. (Japanese)
- Miracle Linux Corporation (Japanese)
- International Business Machines, Corp.
- Oracle Corporation
- iPlanet (Sun Microsystems, Inc.)
- Novell, Inc.
- The SCO Group, Inc. (Caldera International, Inc.)

Revision history

- July 14, 2003: This page is revamped.

- 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

Software Vulnerability Information
Software Division

Update: July 14, 2003

HS02-006;
Vulnerabilities Related to SNMP

Modification in JP1/Cm2/Network Node Manager

In JP1/Cm2/Network Node Manager, a security problem associated with SNMP was found. Please use the following patches to replace your module files.

[Notes]

- In addition to the application of these patches, you also need to apply the patches provided by non-Hitachi vendors for the SNMP problem, if any. Please download the appropriate patches from the vendors' Web sites.
For operating systems other than HP-UX, there is no restriction on the order in which the Hitachi patches and other vendors' patches are applied (you can apply whichever first.).
For HP-UX, follow the patch application procedure for JP1/Cm2/Network Node Manager.
- This problem is corrected in the version 06-71 and later.

● Japanese version

Model	Version	Platform	Patch		Scheduled corrected version	Last update
			Application procedure	Download		
P-2442-6164 P-2442-6264	06-51 - 06-51-/A	Windows 2000 Windows NT	HS02-006-01-a	P-2442-6164_0651SD.exe (1,213,416byte)	06-51-/B	July 14, 2003
P-1B42-6161 P-1B42-6261	06-51	HP-UX	HS02-006-01-b	P-1B42-6161_0651SB.tar (3,870,720byte)	06-51-/A	July 14, 2003
P-9D42-6161 P-9D42-6261	06-51	Solaris	HS02-006-01-c	P-9D42-6161_0651SA.tar (5,187,072byte)	06-51-/A	July 14, 2003

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

P-2442-6194 P-2442-6294	05-20 - 05-20-/F	Windows NT	HS02-006-01-d	P-2442-6194_0520SK.exe (2,256,064byte)	05-20-/G	July 14, 2003
P-1B42-6111 P-1B42-6211	05-20 - 05-20-/E	HP-UX	HS02-006-01-e	P-1B42-6111_0520SH.tar (5,519,360byte)	05-20-/F	July 14, 2003
P-9D42-6111 P-9D42-6211	05-20 - 05-20-/E	Solaris	HS02-006-01-f	P-9D42-6111_0520SC.tar (4,632,064byte)	05-20-/F	July 14, 2003

❖ There are no prerequisite patches related to these patches.

Revision history

- July 14, 2003: This page is revamped.
- September 20, 2002: Security patches for version 05-20 are 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

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

HS02-006;
Vulnerabilities Related to SNMP

Modification in JP1/Cm2/Extensible Agent

In JP1/Cm2/Extensible Agent, a security problem associated with SNMP was found. Please use the following patches to replace your module files.

[Note]

- In addition to the application of these patches, you also need to use the Windows corrective program provided by Microsoft for the SNMP problem. Please download this program from the Microsoft Web site. There is no restriction on the order in which the patches and program are applied (you can apply whichever first.).

● Japanese version

Model	Version	Platform	Patch		Last update
			Application procedure	Download	
P-2442-6A64	06-50 - 06-50-/A	Windows 2000 Windows NT	HS02-006-02-a	P-2442-6A64_0650SA.exe (28,296byte)	July 14, 2003
P-2442-5A94	05-20 - 05-20-/G	Windows 2000 Windows NT	HS02-006-02-b	P-2442-5A94_0520SA.exe (28,296byte)	July 14, 2003

● English version

Model	Version	Platform	Patch		Last update
			Application procedure	Download	
P-2442-6A67	06-50	Windows 2000 Windows NT	HS02-006-02-c	P-2442-6A67_0650SA.exe (28,808byte)	July 14, 2003
P-2442-5A97	05-20	Windows NT	HS02-006-02-d	P-2442-5A97_0520SA.exe (28,808byte)	July 14, 2003

Revision history

- July 14, 2003: This page is revamped.

- 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

Update: July 14, 2003

HS02-006;
Vulnerabilities Related to SNMP

Modification in JP1/Cm2/Extensible SNMP Agent

In JP1/Cm2/Extensible SNMP Agent, a security problem associated with SNMP was found. Please use the following patches to replace your module files.

[Note]

- In addition to the application of these patches, you also need to apply the patches provided by non-Hitachi vendors for the SNMP problem, if any. Please download the appropriate patches from the vendors' Web sites.
  For operating systems other than HP-UX, there is no restriction on the order in which the Hitachi patches and other vendors' patches are applied (you can apply whichever first.).
  When you apply the HP-UX patches, click here to see the precautions.

● Japanese version

Model	Version	Platform	Patch		Last update
			Application procedure	Download	
P-1642-6A6	06-50	HI-UX/WE2	HS02-006-03-a	P-1642-6A6_0650SA.tar (3,727,360byte)	July 14, 2003
P-1B42-6A61	06-50	HP-UX	HS02-006-03-b	P-1B42-6A61_0650SA.tar (1,822,720byte)	July 14, 2003
P-9142-6A61	06-50 - 06-50-/A	AIX	HS02-006-03-c	P-9142-6A61_0650SA.tar (1,720,320byte)	July 14, 2003
P-9D42-6A61	06-50	Solaris	HS02-006-03-d	P-9D42-6A61_0650SA.tar (1,239,040byte)	July 14, 2003
P-9S42-6A61	06-50	Linux	HS02-006-03-e	P-9S42-6A61_0650SA.tar (1,413,120byte)	July 14, 2003
P-9U42-6A61	06-50	Tru64	HS02-006-03-f	P-9U42-6A61_0650SA.tar (1,525,760byte)	July 14, 2003
P-1642-5A1	05-20 - 05-20-/B	HI-UX/WE2	HS02-006-03-g	P-1642-5A1_0520SA.tar (778,240byte)	July 14, 2003
P-1B42-5A11	05-20 - 05-20-	HP-UX	HS02-006-03-h	P-1B42-5A11_0520SA.tar (614,400byte)	July 14, 2003

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

	/C				
P-9142-5A11	05-20 - 05-20-/C	AIX	HS02-006-03-i	P-9142-5A11_0520SA.tar (768,000byte)	July 14, 2003
P-9D42-5A11	05-20 - 05-20-/D	Solaris	HS02-006-03-j	P-9D42-5A11_0520SB.tar (2,088,960byte)	July 14, 2003
P-9S42-5A11	05-20	Linux	HS02-006-03-k	P-9S42-5A11_0520SA.tar (512,000byte)	July 14, 2003

● English version

Model	Version	Platform	Patch		Last update
			Application procedure	Download	
P-1B42-6A62	06-50	HP-UX	HS02-006-03-l	P-1B42-6A62_0650SA.tar (1,822,720byte)	July 14, 2003
P-9142-6A62	06-50	AIX	HS02-006-03-m	P-9142-6A62_0650SA.tar (1,720,320byte)	July 14, 2003
P-9D42-6A62	06-50	Solaris	HS02-006-03-n	P-9D42-6A62_0650SA.tar (1,239,040byte)	July 14, 2003
P-9U42-6A62	06-50	Tru64	HS02-006-03-o	P-9U42-6A62_0650SA.tar (1,525,760byte)	July 14, 2003
P-1B42-5A12	05-20	HP-UX	HS02-006-03-p	P-1B42-5A12_0520SA.tar (614,400byte)	July 14, 2003
P-9142-5A12	05-20	AIX	HS02-006-03-q	P-9142-5A12_0520SA.tar (768,000byte)	July 14, 2003
P-9D42-5A12	05-20	Solaris	HS02-006-03-r	P-9D42-5A12_0520SA.tar (2,088,960byte)	July 14, 2003

Revision history

- July 14, 2003: This page is revamped.

- 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

Update: July 14, 2003

HS02-006;
Vulnerabilities Related to SNMP

Modification in JP1/Cm2/SubManager

In JP1/Cm2/SubManager, a security problem associated with SNMP was found. Please use the following patches to replace your module files.

[Note]

- In addition to the application of these patches, you also need to apply the patches provided by non-Hitachi vendors for the SNMP problem, if any. Please download the appropriate patches from the vendors' Web sites.
For operating systems other than HP-UX, there is no restriction on the order in which the Hitachi patches and other vendors' patches are applied (you can apply whichever first.).
When you apply the HP-UX patches, click here to see the precautions.

● Japanese version

Model	Version	Platform	Patch		Last update
			Application procedure	Download	
P-2442-6B64	06-51	Windows 2000 Windows NT	HS02-006-04-a HS02-006-04-b	P-2442-6B64_0651SA.exe (37,768byte) P-2442-6B64_0651SB.exe (403,064byte)	July 14, 2003
P-2442-6C64					
P-2442-6D64					
P-1642-6B6	06-51	HI-UX/WE2	HS02-006-04-c HS02-006-04-d	P-1642-6B6_0651SA.tar (3,727,360byte) P-1642-6B6_0651SB.tar (675,840byte)	July 14, 2003
P-1642-6C6					
P-1B42-6B61	06-51	HP-UX	HS02-006-04-e HS02-006-04-f	P-1B42-6B61_0651SA.tar (1,822,720byte) P-1B42-6B61_0651SB.tar (624,640byte)	July 14, 2003
P-1B42-6C61					
P-1B42-6D61					
P-1B42-6E61					

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

P-9142-6B61 P-9142-6C61	06-51	AIX	HS02-006-04-g HS02-006-04-h	P-9142-6B61_0651SA.tar (1,720,320byte) P-9142-6B61_0651SB.tar (1,024,000byte)	July 14, 2003
P-9D42-6B61 P-9D42-6C61 P-9D42-6D61 P-9D42-6E61	06-51	Solaris	HS02-006-04-i HS02-006-04-j	P-9D42-6B61_0651SA.tar (1,239,040byte) P-9D42-6B61_0651SB.tar (747,520byte)	July 14, 2003
P-2442-5B94 P-2442-5C94 P-2442-5D94	05-20-/A - 05-20-/B	Windows NT	HS02-006-04-k HS02-006-04-l	P-2442-5B94_0520SA.exe (37,768byte) P-2442-5B94_0520SB.exe (397,112byte)	July 14, 2003
P-1642-5B1 P-1642-5C1	05-20-/A	HI-UX/WE2	HS02-006-04-m HS02-006-04-n	P-1642-5B1_0520SA.tar (778,240byte) P-1642-5B1_0520SB.tar (655,360byte)	July 14, 2003
P-1B42-5B11 P-1B42-5C11 P-1B42-5D11 P-1B42-5E11	05-20-/A	HP-UX	HS02-006-04-o HS02-006-04-p	P-1B42-5B11_0520SA.tar (614,400byte) P-1B42-5B11_0520SB.tar (706,560byte)	July 14, 2003
P-9142-5B11 P-9142-5C11	05-20-/A	AIX	HS02-006-04-q HS02-006-04-r	P-9142-5B11_0520SA.tar (768,000byte) P-9142-5B11_0520SB.tar (1,024,000byte)	July 14, 2003
P-9D42-5B11 P-9D42-5C11 P-9D42-5D11 P-9D42-5E11	05-20-/A - 05-20-/B	Solaris	HS02-006-04-s HS02-006-04-t	P-9D42-5B11_0520SA.tar (2,088,960byte) P-9D42-5B11_0520SB.tar (716,800byte)	July 14, 2003

* Apply both patches whose name ends with SA and SB.

Revision history

- July 14, 2003: This page is revamped.

- 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

| Term of Use | Privacy Notice | About Hitachi |

Update: July 14, 2003

HS02-006;
Vulnerabilities Related to SNMP

Modification in JP1/Cm2/Hierarchical Agent

In JP1/Cm2/Hierarchical Agent, a security problem associated with SNMP was found. Please use the following patches to replace your module files.

[Note]

- In addition to the application of these patches, you also need to apply the patches provided by non-Hitachi vendors for the SNMP problem, if any. Please download the appropriate patches from the vendors' Web sites. There is no restriction on the order in which the patches and program are applied (you can apply whichever first.).

● Japanese version

Model	Version	Platform	Patch		Last update
			Application procedure	Download	
P-2442-6Y64	06-51 - 06-51-/A	Windows 2000 Windows NT	HS02-006 -05-a	P-2442-6Y64_0651SA.exe (51,440byte)	July 14, 2003
P-1B42-6Y61	06-51	HP-UX	HS02-006 -05-b	P-1B42-6Y61_0651SA.tar (92,160byte)	July 14, 2003
P-9D42-6Y61	06-51	Solaris	HS02-006 -05-c	P-9D42-6Y61_0651SA.tar (337,920byte)	July 14, 2003
P-2442-6Y94	05-21	Windows NT	HS02-006 -05-d	P-2442-6Y94_0521SA.exe (49,464byte)	July 14, 2003
P-1B42-6Y11	05-21	HP-UX	HS02-006 -05-e	P-1B42-6Y11_0521SA.tar (81,920byte)	July 14, 2003
P-9D42-6Y11	05-21	Solaris	HS02-006 -05-f	P-9D42-6Y11_0521SA.tar (296,960byte)	July 14, 2003

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

Revision history

- July 14, 2003: This page is revamped.

- 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

Home > Vulnerability Information > Software Vulnerability Information > HS02-006-06

Update: July 14, 2003

HS02-006;
Vulnerabilities Related to SNMP

Vulnerability in the SNMP Agent of Hitachi Directory Server Version 2 (HP-UX)

We found that Hitachi Directory Server Version 2 for HP-UX has been affected by the SNMP security problem (Advisory CA-2002-03) disclosed by the CERT/CC on February 12, 2002.
(Hitachi Directory Server Version 2 includes the SNMP agent that collects statistics of operations performed on the directory server.)
However, this problem only occurs if you make the SNMP-related settings in the Administration Server of Hitachi Directory Server Version 2. If you do not make the settings, no problem occurs because the SNMP agent is inactive.
Also, this security problem does not affect Hitachi Directory Server Version 2 for Windows which uses the SNMP master agent of the operating system. If the use of SNMP is set, apply the Microsoft corrective program.

The SNMP master agent of Hitachi Directory Server Version 2 for HP-UX is located in:

```
  /opt/hitachi/DirectoryServerV2/plugins/snmp/magt/magt
```

Use the `ps` command to check whether the SNMP master agent of Hitachi Directory Server Version 2 exists.

```
Input example

 ps -ef | grep magt




Output Example

 root 13622 13600   0 22:13:03 pts/tb   0:00 grep magt

 root   5938     1  0  Apr  5  ?       1:04 /opt/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

```
/                                            DirectoryServerV2/
                                             plugins/snmp/magt/magt
```

If you have started and use the SNMP agent of Hitachi Directory Server Version 2, do one of the following actions to address the security problem.

1. Only allow SNMP access from permitted hosts.
2. If you started the SNMP master agent of Hitachi Directory Server Version 2 on a system to which a third party may have SNMP access from an external network, stop the SNMP master agent using the following procedure.

   ```
   How to stop
   ```

   ```
     kill -TERM <magt-PID>
   ```

[Supplementary notes]

- Hitachi Directory Server Version 2 does not register the SNMP master agent with the autostart script.
- In the autostart script, delete the registration of

  ```
  /opt/hitachi/DirectoryServerV2/plugins/snmp/magt/magt
  ```

  , if registered.

Substituting Hitachi Directory Server's operation information for SNMP collection information
Hitachi Directory Server Version 2 contains the Administration Server that enables users to reference operation information such as the cache usage for the directory server and the number of connections.
Stopping the SNMP master agent to address the security problem disables the monitoring from the SNMP manager product. Please reference the operation information provided by the Administration Server as alternative information.

- How to reference the operation information for Hitachi Directory Server Version 2
  From the Administration Server TOP window, select the server instance for which you want to reference the operation status, and then click the button. Start the server instance if it has stopped.
  To reference Hitachi Directory Server's operation information, click the **Server Status** button shown in the top of the screen. From the left frame, select the following link to reference the information.
  - Directory server status monitoring window
  - Database status monitoring window

- How to start the Administration Server in HP-UX
  1. Execute the

     ```
     /opt/hitachi/DirectoryServerV2/start-admin
     ```

     command using the superuser's privilege.
     The Administration Server process starts.

2. From the browser, specify `http://`*<server-host-name>*`:`*<port-number>*.
   The dialog box appears, prompting for the user name and password.
3. Specify the administrator's user ID and password. The Administration Server starts.

Revision history

- July 14, 2003: This page is revamped.

- 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

Update: July 14, 2003

HS02-006;
Vulnerabilities Related to SNMP

Note on Using the HP-UX SNMP Patch

When you apply the HP-UX SNMP patch and other OV EMANATE Agent patches to the installation environment for HP OpenView products, there are restrictions due to differences in SNMP between HP-UX and JP1/Cm2. For example, the order in which patches are applied is restricted. These restrictions apply to the following JP1/Cm2 products. The specific order in which patches are applied varies depending on the product.

- JP1/Cm2/Extensible SNMP Agent (referred to as JP1/Cm2/ESA hereinafter)
- JP1/Cm2/SubManager
- JP1/Cm2/Network Node Manager (referred to as JP1/Cm2/NNM hereinafter)

1. **For JP1/Cm2/Extensible SNMP Agent**

   After you uninstall JP1/Cm2/ESA, apply the HP-UX SNMP patch, and then re-install JP1/Cm2/ESA (the definition information is inherited without any change).

   [Note]
   As long as JP1/Cm2/ESA is installed, the SNMP provided by JP1/Cm2/ESA has priority and the SNMP provided by HP-UX is not started.
   However, once you uninstall JP1/Cm2/ESA, the SNMP provided by HP-UX starts.
   To use JP1/Cm2/ESA, be sure to apply the security patch for the SNMP of JP1/Cm2/ESA after reinstalling JP1/Cm2/ESA. If you use a version of JP1/Cm2/ESA for which the security patch is not provided, take preventive measures such as inhibiting SNMP access from unauthorized hosts.

2. **For JP1/Cm2/SubManager**
   Apply either the method in (a) or (b).

   (a) Apply the HP-UX SNMP patch later
   - Apply the security patch for JP1/Cm2/SubManager SNMP.
     If you use a version of JP1/Cm2/SubManager for which the security patch is not provided, take preventive measures such as inhibiting SNMP access from unauthorized hosts.
     At this point, do not apply the HP-UX SNMP patch yet.
   - Then, when you stop the use of JP1/Cm2/SubManager and uninstall it, apply the HP-UX SNMP patch if you want to

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

continue the use of HP-UX.
At this point, apply the HP-UX SNMP patch after uninstalling JP1/Cm2/SubManager.

(b) Immediately apply the HP-UX SNMP patch

- After uninstalling JP1/Cm2/SubManager, apply the HP-UX SNMP patch.
  Then, re-install JP1/Cm2/SubManager. However, you must construct the system from scratch because the JP1/Cm2/SubManager definition information and databases are deleted.
- After re-installing JP1/Cm2/SubManager, be sure to apply the security patch for SNMP for JP1/Cm2/SubManager.
  If you use a version of JP1/Cm2/SubManager for which the security patch is not provided, take preventive measures such as inhibiting SNMP access from unauthorized hosts.

[Note]
For JP1/Cm2/SubManager, you need to delete JP1/Cm2/SubManager before you can apply the HP-UX SNMP patch. In this case, you must construct the system from scratch because the JP1/Cm2/SubManager definition information and databases are deleted. If this causes a problem, apply the method in (a) above. Otherwise, we recommend that you apply the method in (b).
As long as JP1/Cm2/SubManager is installed, the SNMP provided by JP1/Cm2/SubManager has priority and the SNMP provided by HP-UX is not started.
However, once you uninstall JP1/Cm2/SubManager, the SNMP provided by HP-UX starts.

3. **For JP1/Cm2/Network Node Manager**
   Follow the procedure for applying the security patch for JP1/Cm2/Network Node Manager.

Revision history

- July 14, 2003: This page is revamped.

- 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