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

Vulnerabilities Related to DNS Resolver Libraries

On June 28, 2002, the CERT/CC released an advisory about a security problem related to DNS resolver❖ libraries (Advisory CA-2002-19).
Advisory CA-2002-19 identifies buffer overflow issues in implementations of DNS resolver libraries. *These vulnerabilities could be exploited, potentially allowing a remote attacker to cause a denial of service or execute arbitrary code with the execution privileges of the application that is utilizing the DNS resolver.*

❖ DNS resolver
The generic name for client programs that issue queries about host names and IP address information stored on a DNS server

This problem affects the following products from Hitachi Software Division. For the affected products, we will provide information including the problem solution procedure.

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

Corrective actions	Product name	Platform	Last update
HS02-014-01	JP1/Cm2/Extensible SNMP Agent	Linux	July 14, 2003
HS02-014-02	JP1/Agent for Process Management	Linux	July 14, 2003

❖ In this homepage, Job Management Partner 1 is abbreviated as JP1.

Revision history

- July 14, 2003: This page is revamped.

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

HS02-014;
Vulnerabilities Related to DNS Resolver Libraries

Modification in JP1/Cm2/Extensible SNMP Agent DNS Resolver

The Computer Emergency Response Team Coordination Center (CERT/CC) that researches and reports on Internet security released the advisory titled *Buffer Overflows in Multiple DNS Resolver Libraries*. This advisory identifies buffer overflow issues in implementations of the DNS resolver libraries. For details, see Advisory CA-2002-19.

In the Linux version of JP1/Cm2/Extensible SNMP Agent, it was found that the buffer overflow issue was not completely resolved simply by applying the patch for the DNS resolver libraries that are included with the operating system.

1. Phenomenon
A host name, not an IP address, may be used to specify the trap destination in the configuration file, or to specify the node name or agent address in the `snmptrap` or `systemtrap` command. If any of these items is specified with a host name, JP1/Cm2/Extensible SNMP Agent uses the DNS resolver library to acquire the IP address. Receipt of an invalid DNS response to such queries could make the client system vulnerable to execution of arbitrary code or denial of service (DoS).

2. Affected program code numbers and versions, and fixed version releases
Contact your Hitachi support service representative.

Models and versions of JP1/Cm2/Extensible SNMP Agent affected by the vulnerability

- **Japanese version**

Model	Version	Platform	Fixed version	Release time
P-9S42-5A11	05-20	Redhat Linux 5.2 Japanese version	05-20-/A	August 2003 (expected)
P-9S42-6A61	06-00 06-00/A 06-50 06-71	Red Hat Linux 6.1/6.2 Japanese version Red Hat Linux 7.1/7.2 Turbo Linux Server 6.1 Japanese version Red Hat Linux Advanced Server 2.1	06-71-/A	Already released

The vulnerability problem for the `snmptrap` and `systemtrap` commands may occur in the versions 05-20, 06-00, 06-00/A, and 06-50. It does not occur in the version 06-71.

● **Workaround**
You can prevent this availability problem from occurring by using the following measures for the current operations. If a fixed version is not available yet, use the following measures:

(1) If the `trap-dest:` label in `/etc/SnmpAgent.d/snmpd.conf` is specified with a host name, use the following measure:

(a) Open the `/etc/SnmpAgent.d/snmpd.conf` file with a text editor.
Change the host name specified after the `trap-dest:` label to the IP address.

Example
Before change: `trap-dest: host-1`
After change: `trap-dest: 15.2.113.223`

(b) Restart JP1/Cm2/Extensible SNMP Agent to apply the changes that you made to the definition files.
Execute the following command as the superuser:

```
/opt/CM2/ESA/bin/snmpstart
```

(2) If host names are specified as the node name and agent address in the `snmptrap` or `systemtrap` command, use the following measure:
(This problem may occur in the versions 05-20, 06-00, 06-00/A, and 06-50. It does not occur in the version 06-71.)

(a) For the `snmptrap` command
Change the host names specified as the node name and agent address in the `snmptrap` command to IP addresses.

Example when the node name is `host-1` and agent address is `host-2`:
Before change: `snmptrap host-1 "" host-2 6 100 ""`
After change: `snmptrap 15.2.113.223 "" 15.2.113.225 6 100 ""`

(b) For the `systemtrap` command
Change the host names specified as the node name and agent address in the `systemtrap` command to IP addresses.

Example when the node name is `host-1` and agent address is `host-2`:
Before change: `systemtrap -s host-1 host-2 program1 Cri`
After change: `systemtrap -s 15.2.113.223 15.2.113.225 program1 Cri`

Revision history

- July 14, 2003: This page is revamped.

---

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

HS02-014;
Vulnerabilities Related to DNS Resolver Libraries

Modification in JP1/Agent for Process Management DNS Resolver

The Computer Emergency Response Team Coordination Center (CERT/CC) that researches and reports on Internet security released the advisory titled *Buffer Overflows in Multiple DNS Resolver Libraries*. This advisory identifies buffer overflow issues in implementations of the DNS resolver libraries. For details, see Advisory CA-2002-19.

In the Linux version of JP1/Agent for Process Management, it was found that the buffer overflow issue was not completely resolved simply by applying the patch for the DNS resolver libraries that are included with the operating system.

1. Phenomenon
JP1/Agent for Process Management uses DNS resolver libraries to obtain IP addresses when event destination addresses or source addresses are written as host names in a definition file. Receipt of an invalid DNS response to such queries could make the client system vulnerable to execution of arbitrary code or denial of service (DoS).

2. Affected program code numbers and versions, and patch releases
Contact your Hitachi support service representative.

Models and versions of JP1/Agent for Process Management affected by the vulnerability

- **Japanese version**

Model	Version	Platform	Fixed version	Release time
P-9S42-5J11	05-21	Redhat Linux 5.2 Japanese version	05-21-/A	
	06-71-/A 06-71	Red Hat Linux 6.1/6.2 Japanese version Red Hat Linux 7.1/7.2 Turbo Linux Server 6.1 Japanese version Red Hat Linux Advanced Server 2.1	06-71-/B	
				Already

P-9S42-6J61	06-51-/B 06-51-/A 06-51	Red Hat Linux 6.1/6.2 Japanese version Red Hat Linux 7.1/7.2 Turbo Linux Server 6.1 Japanese version	06-51-/C	released
	06-00-/B 06-00-/A 06-00	Red Hat Linux 5.2 Japanese version Red Hat Linux 6.1/6.2 Turbo Linux Server 6.1 Japanese version	06-00-/C	

● **Workaround**

The following workaround may be applied to circumvent this vulnerability, but customers are advised to obtain the patch release as soon as possible.

The buffer overflow issue can be avoided if the event destinations and source addresses are written in definition files as IP addresses rather than as host names.

(1) In destination definition files, write the destinations as IP addresses rather than as host names.

Relevant files

- SNMP agent setup file: `/etc/SnmpAgent.d/snmpd.conf`
- Activation event destination definition file: `/etc/opt/CM2/APM/conf/apmdest.conf`
- JP1/Cm2/Internet SNMP Gateway destination definition file: `/etc/opt/CM2/APM/conf/apmproxy.conf`

Modification procedure

a. SNMP agent setup file

If the trap destination (following the `trap-dest:` label) is a host name, change the host name to an IP address.

Example

Before change: `trap-dest: host-1`

After change: `trap-dest: 15.2.113.223`

b. Activation event destination definition file

If the event destination is a host name, change the host name to an IP address.

c. JP1/Cm2/Internet SNMP Gateway destination definition file

If the JP1/Cm2/Internet SNMP Gateway and monitoring manager destination are written as host names, change the host names to IP addresses.

Example

```
Before change: {host-isg;host-sso1;host-sso2;}
After change: {100.100.100.1;100.100.100.2;100.100.100.3;}
```

(2) In the event notification source address definition file, write the source addresses as IP addresses.

Relevant files

- Event notification source address definition file: `/etc/opt/CM2/APM/conf/apmaddr.conf`

Modification procedure

a. Check the version of the installed JP1/Agent for Process Management program.

The three files listed above were supplied from version 06-51. If you are running an earlier version of JP1/Agent for Process Management, create these files, entering the source addresses as IP addresses as described in *b* below.

b. Specify IP addresses for event source addresses not yet entered in the file.

Write an IP address to set as the event source, followed by a semicolon (;). The address must be recognizable by JP1/Server System Observer.

Example

```
1.1.255.1;
```

(3) Restart JP1/Agent for Process Management to apply the changes that you made to the definition files.

Restart procedure

a. Stop JP1/Agent for Process Management.

Execute `/opt/CM2/APM/bin/apmstop` command.

b. Start JP1/Agent for Process Management.

Execute `/opt/CM2/APM/bin/apmstart` command.

c. Make sure that JP1/Agent for Process Management started successfully.

Run the `ps` command to ensure that the processes (`hiapmmib` and `apmProcMng`) exist and that no error messages were output to the log file (`/var/opt/CM2/APM/log/apmerr.log`).

Revision history

- July 14, 2003: This page is revamped.

Page Top