Update: July 14, 2003

Vulnerabilities Related to SQL Server 2000 and Microsoft Desktop Engine 2000 (MSDE 2000)

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

Corrective actions	Product name	Platform	Last update
HS02-013-01	JP1/VERITAS Backup Exec 9.0 for Windows Servers	Windows	July 14, 2003
HS02-013-02	RealSecure WorkGroup Manager, System Scanner, RealSecure SiteProtector, RealSecure ICEcap Manager	Windows	July 14, 2003
HS02-013-03	JP1/VantagePoint Internet Services	Windows	July 14, 2003

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

■ Details of the problem

On June 29, 2002, the CERT/CC released an advisory about a security problem related to Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 (Advisory CA-2002-22). (Microsoft published Security Bulletin MS02-039 on July 25, 2002 to address these vulnerabilities.)
Advisory CA-2002-22 identifies buffer overrun and denial-of-service vulnerabilities in SQL Server 2000 and its derivative product, MSDE 2000, which is an embedded software component. In addition to SQL Server 2000, software products including MSDE 2000 also have these vulnerabilities.
These vulnerabilities may cause the SQL Server service to terminate abnormally or may cause arbitrary code to run in a security context. They may also cause the system to suffer a denial-of-service attack, significantly degrading system performance.

This problem affects the following products from Hitachi Software Division.

We recommend that you use the following workaround for your system until the patch is applied.

1. Set the network equipment, such as the router, and the server to block communication traffic from insecure hosts to UDP port No. 1434.

Reference information about the Slammer/SQL Exp worm:

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

The Slammer/SQL Exp worm, which has been reported on since about January 25, might infect servers running SQL Server 2000. It was found that the worm might also infect MSDE 2000, a derivative product of SQL Server 2000. This means software products including MSDE 2000 might be infected.
(**CERT Advisory CA-2003-04 MS-SQL Server Worm**)

- For solutions for SQL Server 2000, see the Microsoft Web site.
- Regarding the MSDE 2000-embedded products provided by Hitachi Software Division, this web site provides information about those products that may be affected and patch release information.

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

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

HS02-013;
Vulnerabilities Related to SQL Server 2000 and Microsoft Desktop Engine 2000 (MSDE 2000)

Modification in JP1/VERITAS Backup Exec 9.0 for Windows Servers

JP1/VERITAS Backup Exec 9.0 for Windows Servers uses the English version of Microsoft MSDE 2000 as an internal database component. The SQL Slammer worm, a computer virus that appeared in January 2003, might infect that component. After installing or upgrading JP1/VERITAS Backup Exec 9.0 for Windows Servers, please be sure to take the following action. Also, for the time being, ExecView will not be supported for use with JP1/VERITAS Backup Exec 9.0 for Windows Servers.

1. Affected products (Japanese version)

```
Product name: JP1/VERITAS Backup Exec 9.0 for Windows Servers
              06-72

Model: RT-1V25-K1W110 /K1WS10 /K1WS40 /K1WL10 /K1WU10 /K1WS20
                     /K1WU20 /K1WS30
```

2. Action to take
   Apply the Microsoft-provided patch for the English version of MSDE 2000 to the English version of the MSDE 2000 component installed together with JP1/VERITAS Backup Exec 9.0 for Windows Servers. For details, see the following URL.

   URL for VERITAS Software Corporation information:
   http://seer.support.veritas.com/docs/254245.htm
   (This is a link to the VERITAS Software Corporation web site.)

3. Action procedure

   (1) Download the Microsoft patch (MS02-039) linked to the above VERITAS information page.

   MS02-039 Patch: *Buffer Overruns in SQL Server 2000 Resolution Service Might Enable Code Execution* (`Q323875_SQL2000_SP2_en.EXE`)

(2) Create a work directory on the target system and then store the patch file in the directory.

(3) Double-click the patch file. You are asked about the decompression destination directory. Type or select an appropriate directory and execute decompression. Four files appear.

(4) Stop the SQL service. From the **Program** menu or **Control Panel**, choose **Administrative Tools** and then **Services**. In the Services window, stop the following services if they are running.

MSSQL$BKUPEXEC SQLAgent$BKUPEXEC

(5) Back up the relevant SQL Server files.
Rename *Program-files-folder*`\Microsoft SQL Server\MSSQL$BKUPEXEC\Binn\SSnetlib.dll` to an appropriate name.

(6) Copy the decompressed `ssnetlib.dll` file to *Program-files-folder*`\Microsoft SQL Server\MSSQL$BKUPEXEC\Binn\`.

(7) Restart the system.

(8) Delete the files created in steps (2) and (3) above.

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

HS02-013;
Vulnerabilities Related to SQL Server 2000 and Microsoft Desktop Engine 2000 (MSDE 2000)

Modification in RealSecure

The following describes how to protect the RealSecure products that use SQL Server 2000 or MSDE 2000 (Microsoft Desktop Engine 2000) from the SQL Slammer Worm.

1. Affected models and versions of RealSecure (Japanese version)
1.1 Products that contain MSDE
Models, product names, and versions
R-1V11-RWGMP RealSecure WorkGroup Manager 6.0, 6.5
R-1V11-RWGMSP RealSecure WorkGroup Manager 6.0, 6.5
R-1V11-RSPSP RealSecure WorkGroup Manager Scalability Pack 6.0, 6.5

1.2 Products that require SQL Server 2000 and MSDE 2000
Models, product names, and versions
R-1V11-S2S1P System Scanner 1 device pack 4.0, 4.1, 4.2
R-1V11-S2S5P System Scanner 5 device pack 4.0, 4.1, 4.2
R-1V11-S2S10P System Scanner 10 device pack 4.0, 4.1, 4.2
R-1V11-S2S20P System Scanner 20 device pack 4.0, 4.1, 4.2
R-1V11-S2S30P System Scanner 30 device pack 4.0, 4.1, 4.2
R-1V11-S2S50P System Scanner 50 device pack 4.0, 4.1, 4.2
R-1V11-S2S75P System Scanner 75 device pack 4.0, 4.1, 4.2
R-1V11-S2S100P System Scanner 100 device pack 4.0, 4.1, 4.2
R-1V11-S2S150P System Scanner 150 device pack 4.0, 4.1, 4.2
R-1V11-S2S200P System Scanner 200 device pack 4.0, 4.1, 4.2
R-1V11-RSSPP RealSecure SiteProtector 1.2
R-1V11-BM1P RealSecure ICEcap Manager 1 License 2.6, 3.0, 3.1
R-1V11-BM5P RealSecure ICEcap Manager 5 License 2.6, 3.0, 3.1
R-1V11-BM10P RealSecure ICEcap Manager 10 License 2.6, 3.0, 3.1

2. How to protect against the Microsoft SQL Slammer Worm
Apply the Microsoft-provided service pack for SQL Server 2000 (including the service pack for MSDE).
See the ISS Knowledgebase for details on how to apply the service pack.
URL for the ISS Knowledgebase (Japanese):
http://www.isskk.co.jp/support/index_KB.html

Accessing the above URL, and then click **Knowledgebase** to open the **Search FAQs** page.

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

Use the following conditions to perform a search:
For **Search Text**, enter `030127-000000`.
For **Search By**, from the pulldown menu, choose **Reference number**.

For details on how to apply the patch for SQL Server 2000 (including the patch for MSDE), search the ISS Knowledgebase and then see:
- *2. How do I apply the service pack to SQL Server2000 and MSDE 2000?*
- Accompanying file: `SP_application_method_and_results.pdf`

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

HS02-013;
Vulnerabilities Related to SQL Server 2000 and Microsoft Desktop Engine 2000 (MSDE 2000)

Modification in JP1/VantagePoint Internet Services

1. Affected version (Japanese version)

   P-242C-5264 JP1/VantagePoint Internet Services 06-71

   ❖Versions 06-50 and 06-51 (including their modified versions) are not affected because they do not contain MSDE 2000.

   Note:
   You need not apply this solution (because MSDE 2000 was not installed) if you installed 06-71 either:

   (a) By overwriting 06-51-/A (to update the version), or
   (b) With SQL Server 7 already installed.

   You can use the following procedure to check whether MSDE 2000 is installed:

   > From **Start**, in **Settings**, choose **Control Panel**. Double-click **Administrative Tools**. Then double-click **Services** to open the Services window. Look for the MSSQL$OVOPS service in the list. If it is in the list, MSDE 2000 is installed.

2. Microsoft-provided patch for MSDE 2000

   At first, Hitachi was unsure whether our relevant products were compatible with the Microsoft-provided patch for MSDE 2000 (SP3). It seemed that those products might need their own patch. After checking the operation of the products with the Microsoft-provided patch, we found that they did not need their own patch. It is only necessary to apply the Japanese version of the Microsoft-provided patch (SP3) without any change.

3. Solution

   Apply the Japanese version of MSDE 2000 SP3. You cannot apply the English version. Our products do not have their own patches provided.

Model	Version	Platform	Applicable patch		Last update
			Application procedure	Download	

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-242C-5264	06-71	Windows	HS02-013 -03-a	Microsoft Web site (Japanese)	July 14, 2003

4. Note:
   This solution is applicable as of February 21, 2003. Microsoft provides the patch. In addition to our instructions to apply the patch, be sure to read the Microsoft-provided information about the patch before applying the patch.

Revision history

- July 14, 2003: This page is revamped.
- March 6, 2003: This security information page was published.

- 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