Software Vulnerability Information
Software Division

Update: July 14, 2003

Vulnerabilities in Bytecode Verifier of the Sun Java Runtime Environment and HttpURLConnection of the Sun Java VM

On April 3, 2002, Sun Microsystems, Inc. announced security problems due to a vulnerability in Bytecode Verifier of the Java Runtime Environment (Bulletin 218) and due to a vulnerability in HttpURLConnection of Java VM (Bulletin 216).

The problem discovered in Bytecode Verifier of Java Runtime Environment is a vulnerability that enables the improper use of an untrusted applet to obtain the privilege of a higher-level user.
Exploiting this vulnerability enables Java applets to bypass access restrictions set in the Java applet access area called the sandbox. This can enable the improper operation of Java applets to perform unauthorized actions on a user's computer.

The problem confirmed in Java Runtime Environment is a vulnerability that enables violators to use malicious Java applets to monitor requests to and responses from a proxy server in an environment where the user uses a proxy server.
If the connection to the Internet uses a proxy server, using malicious Java applets to exploit this vulnerability can enable an attacker to transfer user information to a desired destination.

The following products provided by Hitachi Software Division may be affected by the above problem.

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

Corrective actions	Product name	Platform	Last update
HS02-001-01	System Manager - Management Console Version 2.0 02-20 or later	Windows	July 14, 2003
	System Manager - Management Console Version 3.0 03-44-/A or earlier		

Revision history

- July 14, 2003: This page is revamped.

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

- 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

HITACHI
Inspire the Next

| Home | Software | » Security |

Japanese

Search in the Hitachi site by Google
GO
> Advanced search

Home > Vulnerability Information > Software Vulnerability Information > HS02-001-01

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

HS02-001;
Vulnerabilities in Bytecode Verifier of the Sun Java Runtime Environment and HttpURLConnection of the Sun Java VM

Modification in System Manager - Management Console

A security problem related to JRE (Java 2 Runtime Environment) was found in System Manager - Management Console, an optional program product of System Manager. This problem is in the JRE used for the Web management console of System Manager. The console service also provides Web management console functionality, so we request that you uninstall the JRE and then use the console service. If you want to use the Web management console, replace the version of System Manager - Management Console with the corrected version 03-50.

1. Affected range of the JRE

   When you install the JRE included in the System Manager - Management Console product, problems arise related to the JRE vulnerability.
   Note that simply installing System Manager - Management Console does not install the JRE. The problem related to the JRE vulnerability occurs only if you install the JRE manually from the CD-ROM of System Manager - Management Console.

2. Versions of System Manager - Management Console containing the affected JRE

● Japanese version

Product name	Model number	Version
System Manager - Management Console Version 2.0	P-2418-3124	02-20 02-30 02-30-/A
System Manager - Management Console Version 2.0 Upgrade	P-2418-312U	
System Manager - Management Console Version 3.0	P-2418-3134	03-00 03-00-/A 03-10 03-20 03-30 03-30-/A 03-31-/A 03-40 03-42 03-44-/A
System Manager - Management Console Version 3.0 Upgrade	P-2418-313U	

3. Procedure

   From **Add/Remove Programs**, uninstall the JRE installed from the CD-ROM of System Manager - Management Console.
   After installation, you can no longer use the Web management console of System Manager - Management Console, so use the console service that also provides Web management console functionality.
   To use the Web management console, you must use version 03-50 of System Manager - Management Console (released in May 2002). Version 03-50 includes the JRE that has been corrected to solve the vulnerability.

4. Note

   If a product other than System Manager - Management Console is using the JRE, uninstalling the JRE may affect other products. Take special care when uninstalling the JRE. In this case, you must replace the current JRE with a JRE that has been corrected to solve the vulnerability and confirmed to run with the other products.

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