Software Vulnerability Information
Software Division

HITACHI
Inspire the Next

Search in the Hitachi site by Google

> GO

> Advanced search

> TOP

∨ What's New

> Notifications

> Alert

> Software Vulnerability Information

> Links to Security Organizations

Update: July 29, 2005

Problem with Expiration of the Digital Certificate for JCE (Java Cryptography Extension) 1.2.1

- Affected products

Corrective action	Product name	Platform	Last update
HS05-015-01	Cosminexus Web Contents Generator	Windows, HP-UX, Solaris	July 29, 2005

- Problem description

On July 11, 2005, a problem with expiration of the digital certificate for JCE (Java Cryptography Extension) 1.2.1 was announced on the Macromedia General TechNote (Japanese).
A digital certificate, which is used to sign jar files included in the JCE 1.2.1 package, expires at 6:43 on July 28, 2005 (Japanese Standard Time). After this time, JCE 1.2.1 will no longer work correctly.
This expiration might cause problems for the above product because it uses JCE 1.2.1 as a Java framework.

This announcement was released in Japanese on July 6, 2005. For details, see the Japanese Announcement.

Revision history

- July 29, 2005: This page is released.

> 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 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

Update: July 29, 2005

HS05-015;
Problem with Expiration of the Digital Certificate for JCE (Java Cryptography Extension) 1.2.1

<u>Solution for Cosminexus Web Contents Generator (Macromedia JRun)</u>

A digital certificate, which is used to sign jar files included in the Java Cryptography Extension (abbreviated hereafter to JCE) 1.2.1 package, expires at 6:43 on July 28, 2005 (Japanese Standard Time). JCE is used as a JSP/Servlet engine of Cosminexus Web Contents Generator 01-02(*1).
Expiration of this certificate might cause problems for systems that meet one of the following conditions:

- JCE is set as a security provider for providing SSL and Login processing.
- The encryption and decryption functions of JCE are directly used from customer applications.

(*1) Cosminexus Web Contents Generator 01-02 is a component of Cosminexus Version 3 and Version 4, and is an OEM product of Macromedia JRun (abbreviated hereafter to JRun) 3.1.

However, Cosminexus Web Contents Generator 01-00 (OEM of JRun 2.3.3) and 01-01 (OEM of JRun 3.0 Service Pack 2a) are not affected by this problem.

If your system meets one of the above conditions, please download, and replace JCE 1.2.1 with, JCE 1.2.2 from the Sun Microsystems website. For details, see *Affected models and versions* below.

[Affected models and versions]

Set product name		Affected components			Platform	Last update
Cosminexus Products	**Model**	**Component name**	**Model**	**Version**		
	P-24Z4-1D34		RT-12443-1214		Windows NT4.0 / 2000	
	P-24Z4-1D44		RT-12443-1214			
Cosminexus Server -	P-1BZ4-1S31		RT-1V24-21111			

> 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

Product	Model	Program	RT Number	Version	OS	Date
Web Edition	P-1BZ4-1S41		RT-1V24-21111		HP-UX	
	P-9DZ4-1D31		RT-1V24-31111		Solaris	
	P-9DZ4-1D41		RT-1V24-31111		Solaris	
Cosminexus Server - Standard Edition	P-24Z4-1E44	Cosminexus Web Contents Generator	RT-12443-1214	01-02(*1)	Windows NT4.0 / 2000	July 29, 2005
	P-24Z4-1K44		RT-12443-1214			
	P-1BZ4-1T31		RT-1V24-21111		HP-UX	
	P-1BZ4-1T41		RT-1V24-21111			
	P-9DZ4-1E31		RT-1V24-31111		Solaris	
	P-9DZ4-1E41		RT-1V24-31111			
Cosminexus Server - Enterprise Edition	P-24Z4-1F44		RT-12443-1214		Windows NT4.0 / 2000	
	P-1BZ4-1U31		RT-1V24-21111		HP-UX	
	P-9DZ4-1F31		RT-1V24-31111		Solaris	

(*1) Cosminexus Web Contents Generator 01-02 is identical to JRun 3.1.

For the fixed versions and corrective actions, contact your Hitachi support service representative.

Revision history

- July 29, 2005: Information about the problem with expiration of the digital certificate for JCE (Java Cryptography Extension) 1.2.1 is 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

| Term of Use | Privacy Notice | About Hitachi |