Update: July 14, 2003

Vulnerabilities Related to Macromedia JRun

On May 9, 2002, the CERT/CC released an advisory about a security problem related to Macromedia JRun (Advisory CA-2002-14)
This advisory reported that a remotely exploitable buffer overflow exists in Macromedia's JRun 3.0 and 3.1. *This vulnerability may enable an attacker to execute their own code with Web server privileges.* This problem only occurs in JRun connectors for Microsoft IIS.

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
HS02-002-01	Cosminexus Server - Web Edition	Windows	July 14, 2003
	Cosminexus Server - Standard Edition	Windows	
	Cosminexus Server - Enterprise Edition	Windows	

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 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

HS02-002;
Vulnerabilities Related to Macromedia JRun

Modification in Cosminexus (Macromedia JRun)

In Cosminexus products, we found a security problem related to overflow in Macromedia JRun used as a JSP/servlet engine. This problem only occurs in JRun connectors for Microsoft IIS. Download and apply the patch from the Macromedia Web site.

● Japanese version

Product set name		Affected components			Platform	Corrective actions	Last update
Cosminexus products	Model	Component name	Model	Version			
Cosminexus Server - Web Edition	P-24Z4-1D34	Cosminexus Web Contents Generator	RT-12443-1214	01-01(*1) or 01-02(*2)	Windows NT4.0/2000	HS02-002-01-a	July 14, 2003
	P-24Z4-1D44	Cosminexus Web Contents Generator	RT-12443-1214	01-02(*2)	Windows NT4.0/2000		
Cosminexus Server - Standard Edition	P-24Z4-1E44	Cosminexus Web Contents Generator	RT-12443-1214	01-01(*1) or 01-02(*2)	Windows NT4.0/2000		
	P-24Z4-1K44	Cosminexus Web Contents Generator	RT-12443-1214	01-02(*2)	Windows NT4.0/2000		
Cosminexus Server - Enterprise Edition	P-24Z4-1F44	Cosminexus Web Contents Generator	RT-12443-1214	01-01(*1) or 01-02(*2)	Windows NT4.0/2000		

*1 Cosminexus Web Contents Generator 01-01 is JRun 3.0 (or 3.0 SP2a) itself.
*2 Cosminexus Web Contents Generator 01-02 is JRun 3.1 itself.

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