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 > HS04-008

Update: December 16, 2004

Vulnerability of Buffer Overflow in Macromedia JRun

- Affected product

Corrective actions	Product name	Platform	Last update
HS04-008-01	Cosminexus Web Contents Generator	Windows, HP-UX, Solaris	December 16, 2004

- Problem description

A buffer overflow vulnerability was identified in the above product. When malicious users attack this vulnerability, the Web server may shut down.

Revision history

- December 16, 2004: This page 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

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

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

Hitachi Incident Response Team

Update: December 16, 2004

HS04-008;
Vulnerability of Buffer Overflow in Macromedia JRun

Solution for Cosminexus Web Contents Generator(Macromedia JRun)

The following vulnerability was found in Macromedia JRun 3.02a and 3.1 (abbreviated as JRun hereafter) used as the JSP/servlet engines of the Cosminexus Version 3 and 4:

- When running the JRun connector in `verbose=true` mode, a remote attacker can exploit a buffer overflow.

The JRun connector provided by JRun used for communication between the Web server and the JRun has an option called `verbose` to output a detailed communication log.
Macromedia, the supplier of the JRun, reports that a malicious remote user can exploit a buffer overflow and crash the Web server when the `verbose` option is set to `true`.

Please set the `verbose` option of the JRun connector to `false`, or apply the patch available at the Web site of Macromedia. For details, see the corrective action in *Models, versions, and corrective actions*.

[Models, versions, and corrective actions]

Product set name		Affected components			Platform	Corrective actions	Last update
Cosminexus Products	**Model**	**Component name**	**Model**	**Version**			
Cosminexus Server - Web Edition	P-24Z4-1D34		RT-12443-1214	01-01 (*1) or 01-02 (*2)	Windows NT4.0/2000	HS04-008-01-a	
	P-24Z4-1D44		RT-12443-1214	01-02 (*2)			
	P-1BZ4-1S31		RT-1V24-21111	01-01 (*1) or 01-02 (*2)	HP-UX	HS04-008-01-b	
	P-1BZ4-1S41		RT-1V24-21111	01-02 (*2)			

	P-9DZ4-1D31	Cosminexus Web Contents Generator	RT-1V24-31111	01-01 (*1) or 01-02 (*2)	Solaris	HS04-008-01-c	December 16, 2004
	P-9DZ4-1D41		RT-1V24-31111	01-02 (*2)			
Cosminexus Server - Standard Edition	P-24Z4-1E44		RT-12443-1214	01-01 (*1) or 01-02 (*2)	Windows NT4.0/ 2000	HS04-008-01-a	
	P-24Z4-1K44		RT-12443-1214	01-02 (*2)			
	P-1BZ4-1T31		RT-1V24-21111	01-01 (*1) or 01-02 (*2)	HP-UX	HS04-008-01-b	
	P-1BZ4-1T41		RT-1V24-21111	01-02 (*2)			
	P-9DZ4-1E31		RT-1V24-31111	01-01 (*1) or 01-02 (*2)	Solaris	HS04-008-01-c	
	P-9DZ4-1E41		RT-1V24-31111	01-02 (*2)			
Cosminexus Server - Enterprise Edition	P-24Z4-1F44		RT-12443-1214	01-01 (*1) or 01-02 (*2)	Windows NT4.0/2000	HS04-008-01-a	
	P-1BZ4-1U31		RT-1V24-21111	01-01 (*1) or 01-02 (*2)	HP-UX	HS04-008-01-b	
	P-9DZ4-1F31		RT-1V24-31111	01-01 (*1) or 01-02 (*2)	Solaris	HS04-008-01-c	

(*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

- December 16, 2004: Information about the vulnerability of buffer overflow in Macromedia JRun 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