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: June 1, 2007

Multiple Vulnerabilities in SSL/TLS Implementations

- Affected product

Corrective actions	Product name	Platform	Last update
HS03-007-01	Hitachi Web Server	HP-UX 10.20/11.0/11i, Solaris 2.6/7/8/9, AIX5L V5.1/V5.2, Linux, Windows NT4.0/2000	June 1, 2007

- Problem description

  On October 1, 2003, CERT/CC released multiple vulnerabilities in SSL/TLS implementations (CA-2003-26).

  These vulnerabilities occur primarily in Abstract Syntax Notation One (ASN.1) parsing code. The most serious vulnerabilities result in denial of service and may allow a remote attacker to execute arbitrary code.

Revision history

- June 1, 2007: The solution for Hitachi Web Server page is updated.
- October 21, 2004: The solution for Hitachi Web Server page is updated.
- August 31, 2004: The solution for Hitachi Web Server page is updated.
- December 22, 2003: The solution for Hitachi Web Server page is updated.
- November 21, 2003: 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

©Hitachi,Ltd. 1994,2008.All rights reserved.

Update: June 1, 2007

HS03-007;
Multiple Vulnerabilities in SSL/TLS Implementations

Solution for Hitachi Web Server

Multiple vulnerabilities in SSL/TLS implementations have been found in Hitachi Web Server.
We are preparing fixed versions of the affected products, and will announce them on this page when they are completed. Please immediately apply the fixed version to your system after the version becomes available.

[Influence]

When SSL functions of Hitachi Web Server are used, server processes or server threads that are attacked due to these vulnerabilities will terminate abnormally. However, this does not allow a remote attacker to execute arbitrary code.

- **Unix version**
  The Unix version uses multi-processes so when a server process is attacked and terminates abnormally, the other processes are not affected and the Web server processing is continued without denial of service.
- **Windows version**
  In the Windows version, when a server thread is attacked, not only the server thread but the server process will terminate abnormally. Service will be temporarily denied, but the server process will be automatically rebooted, so the system will recover from the denial of service.

[Workaround]

If SSL functions of Hitachi Web Server are used, no workaround exists.

[Affected models, versions and fixed versions]

Model	Version	Platform	Fixed version	Release Time	Last Update
P-1B41-E111	01-00 - 01-00-/B, 01-01 - 01-01-/D, 01-02 - 01-02-/D	HP-UX 10.20	(*4)		November 21, 2003
P-1B41-E121	01-00 - 01-00-/B, 01-01 - 01-01-/D, 01-02 - 01-02-/D	HP-UX 11.0/11i	(*5)		June 1, 2007

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-1B41-E121B1	01-00 - 01-00-/A, 01-01 - 01-01-/A, 01-02 - 01-02-/D	HP-UX 11.0/11i	(*5)		June 1, 2007
P-1B41-E151	02-00, 02-02	HP-UX 11.0/11i	02-02-/A (*3)	November 30, 2004	June 1, 2007
P-9D41-E111	01-00 - 01-00-/B	Solaris 2.6/7	(*1)		October 21, 2004
	01-01 - 01-01-/D	Solaris 2.6/7/8			
	01-02 - 01-02-/D	Solaris 2.6/7/8/9			
P-9D41-E151	02-00	Solaris 2.6/7/8/9	02-02 (*3)	September 15, 2004	October 21, 2004
P-1M41-E111	01-01 - 01-01-/D	AIX5L V5.1	(*2)		October 21, 2004
	01-02 - 01-02-/E	AIX5L V5.1/V5.2			
P-1M41-E151	02-00 - 02-00-/A	AIX5L V5.1/V5.2	02-02 (*3)	April 30, 2004	August 31, 2004
P-9S41-E111	01-01 - 01-01-/D	Turbo Linux 6.1 (Japanese version), RedHat Linux 6.2 (Japanese version)	(*4)		November 21, 2003
P-9S41-E151	02-00	Red Hat Linux 7.2, Red Hat Enterprise Linux AS Ver2.1	02-00-/A	December 10, 2003	December 22, 2003
P-1L41-E111	01-01	Turbolinux Server 6 for MP Series	(*4)		November 21, 2003
P-1L41-E151	02-00	Turbolinux 7 Server for AP8000	(*4)		November 21, 2003
P-2441-E151	02-00 - 02-00-/C, 02-00-A, 02-00-B - 02-00-BA, 02-01 - 02-01-/A, 02-03 - 02-03-/A	Windows NT 4.0 Workstation/Server, Windows 2000 Server/Advanced Server/Datacenter Server	02-04 (*3)	November 30, 2004	June 1, 2007

(*1) Please upgrade the version to 02-02 of model P-9D41-E151 or later.

(*2) Please upgrade the version to 02-02 of model P-1M41-E151 or later.

(*3) Please upgrade the version to a fixed revision.

(*4) Please contact your Hitachi support service representative.

(*5) Please upgrade the version to 02-02-/A of model P-1B41-E151 or later.

These vulnerabilities also affect the Hitachi Web Server included in the following Cosminexus Server products.

Cosminexus product	Model	Version	Model included in Cosminexus	Last Update
Cosminexus Server - Web Edition	P-1BZ4-1S31	03-00 or later	P-1B41-E121	November 21, 2003
	P-9DZ4-1D31	03-00 or later	P-9D41-E111	November 21, 2003
Cosminexus Server - Standard Edition	P-1BZ4-1T31	03-00 or later	P-1B41-E121	November 21, 2003
	P-9DZ4-1E31	03-00 or later	P-9D41-E111	November 21, 2003
	P-	03-00		November

Cosminexus Server - Enterprise Edition	1BZ4-1U31	or later	P-1B41-E121	21, 2003
	P-9DZ4-1F31	03-00 or later	P-9D41-E111	November 21, 2003
Cosminexus Server - Web Edition Version 4	P-1BZ4-1S41	04-01 or later	P-1B41-E121	November 21, 2003
	P-9DZ4-1D41	04-01 or later	P-9D41-E111	November 21, 2003
Cosminexus Server - Standard Edition Version 4	P-1BZ4-1T41	04-01 or later	P-1B41-E121	November 21, 2003
	P-9DZ4-1E41	04-01 or later	P-9D41-E111	November 21, 2003
	P-1MZ4-1E41	04-01 or later	P-1M41-E111	November 21, 2003
Cosminexus Application Server Version 5	P-1B43-1B51	05-00 or later	P-1B41-E121	November 21, 2003
		05-05 or later	P-1B41-E151	November 21, 2003
	P-1M43-1B51	05-00 or later	P-1M41-E111	November 21, 2003
		05-05 or later	P-1M41-E151	November 21, 2003
	P-2443-1D54	05-01 or later	P-2441-E151	November 21, 2003
Cosminexus Developer Version 5	P-2443-1F54	05-01 or later	P-2441-E151	November 21, 2003
Embedded Cosminexus Server Base Version 5	P-2443-1G54	05-05 or later	P-2443-E151	August 31, 2004
Cosminexus Application Server Standard Version 6	P-1B43-1D61	06-00 or later	P-1B41-E151	August 31, 2004
Cosminexus Application Server Enterprise Version 6	P-1B43-1K61	06-00 or later	P-1B41-E151	August 31, 2004
Cosminexus Developer Light Version 6	P-2443-1A64	06-00 or later	P-2443-E151	August 31, 2004
Cosminexus Developer Standard Version 6	P-2443-1B64	06-00 or later	P-2443-E151	August 31, 2004
Cosminexus Developer Professional Version 6	P-2443-1F64	06-00 or later	P-2443-E151	August 31, 2004

Cosminexus Application Server Standard Version 6	P-2443-1D64	06-00 or later	P-2443-E151	August 31, 2004
Cosminexus Application Server Enterprise Version 6	P-2443-1K64	06-00 or later	P-2443-E151	August 31, 2004
Cosminexus Primary Server Version 6	P-2443-1C64	06-00 or later	P-2443-E151	August 31, 2004
Cosminexus Primary Server Base Version 6	P-2443-1P64	06-00 or later	P-2443-E151	August 31, 2004

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

Revision history

- June 1, 2007: Information about fixed versions of P-1B41-E121, P-1B41-E121B1, P-1B41-E151, and P-2441-E151 is updated.
  (*5) is added.
- October 21, 2004: Information about fixed versions of P-9D41-E111, P-9D41-E151 and P-1M41-E111 is updated.
- August 31, 2004: Versions of models P-1B41-E151, P-1M41-E151 and P-2441-E151 are added to Affected models, versions and fixed versions. The fixed versions of P-9D41-E111, P-9D41-E151, P-1M41-E111 and P-1M41-E151 are available.
  Models of Cosminexus products are added.
- December 22, 2003: The corrected version of P-9S41-E151 02-00 is available.
- November 21, 2003: 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

©Hitachi,Ltd. 1994,2008.All rights reserved.