Update: June 14, 2005

Vulnerability Issues in Implementations of the S/MIME Protocol

- Affected product

Corrective actions	Product name	Platform	Last update
HS03-006-01	PKI Runtime Library	Windows 95/98/Me/NT/2000/XP, Solaris 8	June 14, 2005
	PKI Developer's Toolkit		
	PKI Runtime Library for Windows Server	Windows NT/2000	
	PKI Runtime Library for HP-UX	HP-UX 11.00/11.11	
	PKI Developer's Toolkit for HP-UX		
	PKI Runtime Library for AIX	AIX 5.1	
	PKI Developer's Toolkit for AIX		
	Groupmax Mail - Security Option Version 6	Windows 98/Me/NT/2000/XP	

- Problem description

  The vulnerabilities were discovered using a test suite constructed by NISCC. When a digital signature of S/MIME is invalid, the behaviour of the application that received the signature is unpredictable.

  The impact on the above Hitachi products is limited to denial of service.

Revision history

- June 14, 2005: Corrective actions page is updated.
- February 25, 2004: Corrective actions page is updated.
- January 19, 2004: Corrective actions page is updated.
- November 12, 2003: Product information is updated, and the fixed version page is linked.

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

- November 6, 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

Update: June 14, 2005

HS03-006;
Vulnerability Issues in Implementations of the S/MIME Protocol

Solution for PKI Runtime Library and Groupmax Mail - Security Option

Vulnerability issues in implementations of the S/MIME protocol have been found in PKI Runtime Library and Groupmax Mail - Security Option.
As for the corrected versions, contact your Hitachi support service representative.

Model	Product name	Version	Platform	Fixed version	Release time	Last update
P-2465-9414	PKI Runtime Library	01-00 - 03-02-/A	Windows 95/98/Me/NT/2000/XP	03-03	January 15, 2004	January 19, 2004
P-2465-9314	PKI Developer's Toolkit	01-00 - 03-02-/A	Windows 95/98/Me/NT/2000/XP	03-03	January 15, 2004	January 19, 2004
P-2465-9614	PKI Runtime Library for Windows Server	02-03 - 03-02-/A	Windows NT/2000	03-03	January 15, 2004	January 19, 2004
P-1B44-7411	PKI Runtime Library for HP-UX	02-02 - 03-02	HP-UX 11.00/11.11	(*1)		June 14, 2005
P-1B44-7311	PKI Developer's Toolkit for HP-UX	02-02 - 03-02	HP-UX 11.00/11.11	(*1)		June 14, 2005
P-9D44-7411	PKI Runtime Library	03-00 - 03-02-/A	Solaris 8	03-03	January 15, 2004	January 19, 2004
P-9D44-7311	PKI Developer's Toolkit	03-00 - 03-02-/A	Solaris 8	03-03	January 15, 2004	January 19, 2004
P-1M44-7411	PKI Runtime Library for AIX	03-02	AIX 5.1	(*1)		June 14, 2005
P-1M44-7311	PKI Developer's Toolkit for AIX	03-02	AIX 5.1	(*1)		June 14, 2005
P-	Groupmax Mail -				January	

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security
@itg.hitachi.co.jp

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

2646-8W44	Security Option Version 6	06-00 - 06-02	Windows 98/Me/NT/2000/XP	06-02-/A	30, 2004	February 25, 2004

(*1) For the fixed versions, contact your Hitachi support service representative.

Revision history

- June 14, 2005: Information about fixed versions of P-1B44-7411, P-1B44-7311, P-1M44-7411, P-1M44-7311 is updated.
- February 25, 2004: The corrected version of P-2646-8W44 is available.
- January 19, 2004: The corrected versions of P-2465-9414, P-2465-9314, P-2465-9614, P-9D44-7411, P-9D44-7311 are available.
- November 12, 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