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

Update: December 26, 2003

Verisign Class 3 and Class 2 PCA Root Certificate Expiration

- Problem description

  A Class 3 and Class 2 Verisign PCA root certificate included in various releases of the SDK and JRE (see Contributing Factors below) will expire on January 7(GMT), 2004 and may result in the following upon expiration:

  1.Java applications and applets, deployed with the Java Plug-in or Java Web Start which authenticate using certificates issued by the expiring root certificates may encounter a security warning dialog box indicating an authentication failure.

  2.Java applications or applets using a Java Secure Socket Extension (JSSE) TrustManager that do not recognize expired root certificates may not be able to access web sites via https.

  For more information, please refer to the following:
  SUN: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57436-1
  IBM: http://www-106.ibm.com/developerworks/java/jdk/security/
  HP: http://www.hp.com/products1/unix/java/infolibrary/verisign.html

Revision history

- December 26, 2003: This page is released.

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