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: July 14, 2003

Vulnerability of Buffer Overflow in Sendmail

CA-2003-12 (Buffer Overflow in Sendmail), which was released by CERT/CC in the U.S., causes the following effects on HI-UX/WE2.

Overview

A buffer overflow vulnerability problem in Sendmail was identified. The following information releases warn that a third party might exploit this vulnerability and remotely acquire the root privilege.

CERT/CC:	CERT Advisory CA-2003-12 Buffer Overflow in Sendmail
JPCERT/CC:	JPCERT/CC Alert 2003-03-31 Another Vulnerability of sendmail

Modification in HI-UX/WE2

As for sendmail 8.8.7, which is delivered with HI-UX/WE2/BASE 06-10 or later (or 07-10 or later), the overflow in question is not a security hole, on the contrary to the general warnings given in the above information releases.
Although this is not a security problem, this buffer overflow may cause child sendmail daemon processes to terminate abnormally (core dump). However, such abnormal termination occurs only in child processes that handled invalid e-mail messages and does not affect parent sendmail daemon processes. The system can continue to process subsequently received e-mail messages if they are valid messages. This buffer overflow problem does not lead to illegal acquisition of the root privilege.
We plan to fix the program to prevent this abnormal termination of child processes in a future revision. We plan to release the latest revision of V-R (06-30, 07-50) at the end of May 2003.
If you are using a HI-UX/WE2/BASE version that is older than 06-10 (or 07-10), please upgrade your system to HI-UX/WE2/BASE 06-10 or later (or 07-10 or later), which includes sendmail 8.8.7.

The latest versions as of this writing are as follows:

Product name	Model	Version
HI-UX/WE2/BASE	P-1611-111	06-30-/D
HI-UX/WE2/BASE	P-1611-112	06-30-/D
HI-UX/WE2/BASE	P-1611-113	07-50-/D

Revision history

- July 14, 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