CERT Advisory CA-1991-03 Unauthorized Password Change Requests Via Mail Messages

Original issue date: April 4, 1991
Last revised: September 18, 1997
Attached copyright statement

A complete revision history is at the end of this file.

I. Description

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received a number of incident reports concerning the receipt of mail instructing the user to immediately change his/her password. The user is further instructed to change the password to one that is specified in the mail message.

These mail messages can be made to look as if they have been sent from a site administrator or root. In reality, they may have been sent by an individual at a remote site, who is trying to gain access to the local machine via the user's account.

Several variations of these mail messages are circulating via the Internet community. We are including one such example at the end of this advisory.

II. Impact

An intruder can gain access to a system through the unauthorized use of the (possibly privileged) accounts whose passwords have been changed.

II. Solution

The CERT/CC recommends the following actions:

1. Any user receiving such a message should verify its authenticity with his/her system administrator before acting on the instructions within the mail message. If a user has changed his/her password per the instructions, he/she should immediately change it again to a secure password and alert his/her system administrator.
2. System administrators should check with their user communities to ensure that no user has changed his/her password in response to one of these mail messages. If this has occurred, immediately have the password changed again. Further, the system should be carefully examined for damage, or changes that may have been caused by the intruder. We also ask that you please contact the CERT/CC.
3. The CERT/CC recommends that system administrators NEVER mail such a request to a user. That is, NEVER send a request for a password change to a user and also specify the new password that should be used.

SAMPLE MAIL MESSAGE as received by the CERT (including spelling errors, etc.)

```
:

{mail header which may or may not be local}

:
```

This is the system administration:

Because of security faults, we request that you change your password to "systest001". This change is MANDATORY and should be done IMMEDIATLY. You can make this change by typing "passwd" at the shell prompt. Then, follow the directions from there on.

Again, this change should be done IMMEDIATLY. We will inform you when to change your password back to normal, which should not be longer than ten minutes.

Thank you for your cooperation,

The system administration (root)

END OF SAMPLE MAIL MESSAGE

Revision History

```
September 18,1997  Attached Copyright Statement
```