CERT Advisory CA-1990-11 Security probes from Italy

Original issue date: December 10, 1990
Last revised: September 17, 1997
Attached copyright statement

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

Many sites on the Internet received messages from "miners@ghost.unimi.it " (131.175.10.64) on Sunday, December 9. The messages stated that "miners" is a group of researchers and students in the computer science department at the state university of Milano in Italy; a group testing for a "common bug" in network hosts. In addition to the messages, a number of sites detected probes from the unimi.it domain. Later today, a number of individuals received a follow up message from "postmaster@ghost.unimi.it " explaining the activities.

We have received reports that this activity has now stopped, and an unofficial explanation has been provided by several administrators at the University of Milano. The rest of this message describes the sequence of events and the security holes that were probed.

Following the original messages from miners@ghost and postmaster@ghost, another message was sent on the afternoon of December 10th from several administrators at the University of Milano. They stated that the authorities at the University had been informed and that the attempts had stopped. They also noted that they had not been informed of the tests in advance.

The administrators at the University of Milano have sent us a copy of the scripts that were used to probe the Internet sites. These scripts checked for the existence of the sendmail WIZ and DEBUG commands, and attempted to get /etc/motd and/or /etc/passwd via TFTP and by exploiting an old vulnerability in anonymous FTP. The scripts also attempted to rsh to a site and try to cat /etc/passwd. Finally, the scripts mailed to root at each site they tested with the message from "miners@ghost.unimi.it ".

The administrators at the University of Milano state that the group that did this was doing this to discover which (if any) sites might have had these security flaws, and then to let the sites know about these vulnerabilities. They have stated that they still intend to inform sites that have these vulnerabilities.

To our knowledge, no site was actually broken into (as of December 10, 1990). Nonetheless, CERT* does not condone this type of activity.

Most of the information in this advisory is based on information given to us via e-mail from individuals at the University of Milano. We have not yet been able to check this information with any officials at the University; if we learn of any other significant information, we will update this advisory.

Revision History

```
September 17,1997  Attached Copyright statement
```