CERT Advisory CA-1991-12 Trusted Hosts Configuration Vulnerability

Original issue date: August 22, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the configuration of several system files. This advisory discusses a workaround since there are no permanent patches available at this time.

This vulnerability is present in a very large number of UNIX-based operating systems. Therefore, we recommend that ALL sites take the corrective actions listed below.

I. Description

The presence of a '-' as the first character in /etc/hosts.equiv, /etc/hosts.lpd and .rhosts files may allow unauthorized access to the system.

II. Impact

Remote users can gain unauthorized root access to the system.

III. Solution

Rearrange the order of entries in the hosts.equiv, hosts.lpd, and .rhosts files so that the first line does not contain a leading '-' character.

Remove hosts.equiv, hosts.lpd, and .rhosts files containing only entries beginning with a '-' character.

.rhosts files in ALL accounts, including root, bin, sys, news, etc., should be examined and modified as required. .rhosts files that are not needed should be removed.

Please note that the CERT/CC strongly cautions sites about the use of hosts.equiv and .rhosts files. We suggest that they NOT be used unless absolutely necessary.

The CERT/CC wishes to thank Alan Marcum, NeXT Computer, for bringing this security vulnerability to our attention. We would also like to thank CIAC for their assistance in testing this vulnerability.

Revision History

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