CERT Advisory CA-1993-01 Revised Hewlett-Packard NIS ypbind Vulnerability

Original issue date: January 13, 1993
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file. **THIS IS A REVISED CERT ADVISORY.**
IT CONTAINS NEW INFORMATION REGARDING AVAILABILITY OF IMAGE KITS
SUPERSEDES CERT ADVISORY CA-92.17

The CERT Coordination Center has received information concerning a vulnerability in the NIS ypbind module for the Hewlett-Packard (HP) HP/UX Operating System for series 300, 700, and 800 computers.

HP has provided revised patches for all of the HP/UX level 8 releases (8.0, 8.02, 8.06, and 8.07). This problem is fixed in HP/UX 9.0. The following patches have been superseded:

Patch ID	Replaced by Patch ID
PHNE_1359	PHNE_1706
PHNE_1360	PHNE_1707
PHNE_1361	PHNE_1708

All HP NIS clients and servers running ypbind should obtain and install the patch appropriate for their machine's architecture as described below.

I. Description

A vulnerability in HP NIS allows unauthorized access to NIS data.

II. Impact

Root on a remote host running any vendor's implementation of NIS can gain root access on any local host running HP's NIS ypbind. Local users of a host running HP's NIS ypbind can also gain root access.

III. Solution

1. All HP NIS clients and servers running ypbind should obtain and install the patch appropriate for their machine's architecture.
   These patches contain a version of ypbind that only accepts ypset requests from a superuser port on the local host. This prevents a non-superuser program from sending rogue ypset requests to ypbind. They also include the mod from the superseded patches which prevented a superuser on a remote system from issuing a ypset -h command to the local system and binding the system to a rogue ypserver.

   These patches may be obtained from HP via FTP (this is NOT anonymous FTP) or the HP SupportLine. To obtain HP security patches, you must first register with the HP SupportLine. The registration instructions are available via anonymous FTP at cert.org (192.88.209.5) in the file "pub /vendors/hp/supportline_and_patch_retrieval".

   The new patch files are:

```
Architecture Patch ID   Filename                                Checksum
------------ --------   --------                                --------
Series 300   PHNE_1706  /hp-ux_patches/s300_400/8.X/PHNE_1706  38955 212
Series 700   PHNE_1707  /hp-ux_patches/s700/8.X/PHNE_1707        815 311
Series 800   PHNE_1708  /hp-ux_patches/s800/8.X/PHNE_1708      56971 299
```

2. The instructions for installing the patch are provided in the PHNE_xxxx.text file (this file is created after the patch has been unpacked).

   The checksums listed above are for the patch archive files from HP. Once unpacked, each shell archive contains additional checksum information in the file "patchfilename.text". This checksum is applicable to the binary patch file "patchfilename.updt".

If you have any questions about obtaining or installing the patches, contact the USA HP SupportLine at 415-691-3888, or your local HP SupportLine number. Please note that the telephone numbers in this advisory are appropriate for the USA and Canada.

The CERT Coordination Center wishes to thank Brian Kelley of Ford Motor Company for bringing this vulnerability to our attention. We would also like to thank Hewlett-Packard for their response to this problem.

Revision History

```
September 19,1997  Attached Copyright Statement
```