CERT Advisory CA-1991-23 Hewlett Packard/Apollo Domain /OS crp Vulnerability

Original issue date: December 18,1991
Last revised: September 18, 1997

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 crp facility in Hewlett Packard/Apollo Domain/OS. This vulnerability is present on all HP/Apollo Domain/OS SR10 systems up through SR10.3. Patches that address this problem will be available in the SR10.3 patch tape (~Feb 92) and in the SR10.4 software release. Contact your local sales office for more information.

I. Description

There is a security problem with the /usr/apollo/bin/crp facility. A user who is not running crp is not vulnerable to this problem.

II. Impact

A person at a remote or local site can obtain the privileges of the user who is running crp.

III. Workaround

The suggested workaround is to disable two system calls that are made by /usr/apollo/bin/crp. The following steps should be executed by root or another appropriate userid that has the privilege to write in the directories involved.

1. Create a file "crplib.c" containing the four-line C program:

```
extern void pad_$dm_cmd(void);
void pad_$dm_cmd() { }
extern void pad_$def_pfk(void);
void pad_$def_pfk() { }
```

1. Compile this program using '-pic':

```
(AEGIS)  /com/cc crplib.c -pic
(UNIX)   /bin/cc -c crplib.c -W0,-pic
```

1. Copy the result to somewhere accessible to all users (/lib/crplib is recommended).

```
(AEGIS)  /com/cpf crplib.bin /lib/crplib
(AEGIS)  /com/edacl -p root prwx -g wheel rx -w rx /lib/crplib

(UNIX)   /bin/cp crplib.o /lib/crplib

(UNIX)   /bin/chmod 755 /lib/crplib
```

1. a) Ensure that all users do an 'inlib' of that file before running crp.
   One way to ensure this would be to replace the /usr/apollo/bin/crp command by a shell script that does the inlib. Doing this step will force crp to use the null functions defined in step 1 above.

```
(AEGIS)  /com/chn /usr/apollo/bin/crp crp.orig
(UNIX)   /bin/mv /usr/apollo/bin/crp /usr/apollo/bin/crp.orig
```

b) Create the file /usr/apollo/bin/crp containing the shell script:

```
(AEGIS)        #!/com/sh
  /com/sh -c inlib /lib/crplib ';' /usr/apollo/bin/crp.orig ^*
(UNIX)        #!/bin/sh
        inlib /lib/crplib
        exec /usr/apollo/bin/crp.orig "$@"
```

c) Make this script executable.

```
(AEGIS)        /com/edacl -p root prwx -g wheel rx -w rx /usr/apollo/bin/crp
(UNIX)        /bin/chmod 755 /usr/apollo/bin/crp
```

NOTE: This workaround will prevent crp from making use of the two system calls; and therefore, it may affect the functionality of various software programs since they will be unable to define programmable function keys, create new windows on the client node, or execute background processes using the Display Manager interface.

The CERT/CC wishes to thank Paul Szabo of the University of Sydney for bringing this problem to our attention and providing a workaround. We would also like to thank Jim Richardson of the University of Sydney for his assistance and Hewlett Packard/Apollo for their timely response to the report of this vulnerability.

Revision History

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