linux-pam: pam_setquota.so vulnerability facilitated through fusermount setuid-root program

From: Matthias Gerstner <mgerstner () suse de>
Date: Thu, 4 Jun 2020 14:28:11 +0200

```
During a review of newly added PAM modules in the linux-pam project [1]
I found a vulnerability [2] in the pam_setquota.so module.

Vulnerability Description
=========================

The pam_setquota module iterates over all mounted file systems using
`setmntent()` and `getmntent()`. It tries to find the longest match of a
file system mounted on /home/$USER or above (except when the explicit
fs=/some/path parameter is passed to the pam module).

The home directory /home/$USER is owned by the unprivileged user,
however. There exist tools like `fusermount` from libfuse which is by
default installed setuid-root for everybody. `fusermount` allows
unprivileged users to mount a FUSE file system using an arbitrary
source device name.

Thus given the following precondition:

1) there is only the root file system (/) or a file system is mounted on
   /home, but not on /home/$USER.

a non-privileged attacker can achieve the following:

2) the attacker mounts a fake FUSE file system over its own home directory:

  ```
  user $ export _FUSE_COMMFD=0
  user $ fusermount $HOME -ononempty,fsname=/dev/sda1
  ```

  This will result in a mount entry in /proc/mounts looking like this:

  ```
  /dev/sda1 on /home/user type fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=100)
  ```

3) when the attacker now logs in with pam_setquota configured then
   pam_setquota will identify /dev/sda1 as the file system to apply the
   user's quota on.

As a result an unprivileged user has full control over onto which block
device the quota is applied.

Consequences Regarding `fusermount`
===================================

It seems that developers find it suprising that regular user accounts
can specify arbitrary source device names in mount entries. It would be
desirable to apply restrictions on the source device string in the
`fusermount` setuid-root tool. It will probably be difficult to
implement this in a backward-compatible and safe way, however.

Bugfix
======

This issue is fixed via upstream commit
27ded8954a1235bb65ffc9c730ae5a50b1dfed61 [3].

Vulnerability Reporting
=======================

This finding was reported privately to upstream. Since the
pam_setquota.so PAM module was never part of an official release no
embargo was setup. For this reason I also did not request a CVE for the
issue.

[1]: https://github.com/linux-pam/linux-pam.git
[2]: https://bugzilla.suse.com/show_bug.cgi?id=1171721
[3]: https://github.com/linux-pam/linux-pam/commit/27ded8954a1235bb65ffc9c730ae5a50b1dfed61

Cheers

Matthias

--
Matthias Gerstner <matthias.gerstner () suse de>
Dipl.-Wirtsch.-Inf. (FH), Security Engineer
https://www.suse.com/security
Phone: +49 911 740 53 290
GPG Key ID: 0x14C405C971923553

SUSE Software Solutions Germany GmbH
HRB 36809, AG Nürnberg
Geschäftsführer: Felix Imendörffer
```

Attachment: signature.asc
Description:

By Date By Thread

Current thread:

linux-pam: pam_setquota.so vulnerability facilitated through fusermount setuid-root program *Matthias Gerstner (Jun 04)*