

Re: nis : how to avoid user1 becoming user2 using local root ?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2004-04/0012.html>

From: Frank Burkhardt (*fbo2_at_gmx.net*)

Date: 04/03/04

Date: Sat, 3 Apr 2004 07:46:36 +0200

To: focus-linux@securityfocus.com

Hi,

On Thu, Apr 01, 2004 at 10:10:48AM -0800, Mike Hogsett wrote:

>
> > *to everyone. The problem is the NFS-server trusting UIDs on remote*
> > *computers.*
>
> *If person-1 is the only one on host-a (e.g. if there is a one to one*
> *mapping between the nfs client and the user) you can perform all_squashing*
> *and anonuid and anongid mapping.*
[snip]
> *So no matter what UID comes in from the NFS client the NFS server will map*
> *them to another user/group id. So who cares if Joe su's to Mark, from*
> *Joe's machine the NFS server will still treat him as Joe.*

Of course the server's administrator can lock UIDs to special machines. This means changing the needed "credential" from (uid) to (uid , ip_address) or (uid, numerical_ip(user's_host(username(uid)))). user's_host(...) is a "function" which can be easily calculated by "username(uid)"'s colleagues.
-> The credential is publicly known.

Everything an "attacker" has to do is changing the ip address of the machine he has root access to (hoping that the machine which really uses the ip is offline or inactive).

Does the uid-to-machine-lock prevent root-users from accidentally changing to arbitrary UIDs? Yes, definitely.

But removing

```
auth sufficient pam_rootok.so
```

from /etc/pam.d/su does the same and it's easier to maintain than a huge /etc/exports on every NFS-server.

SecurityFocus Linux: Re: nis : how to avoid user1 becoming user2 using local root ?

Real attacks can only be prevented by a network file system which servers require credentials that are not publicly known.

Frank