

Re: Samba 3.x + kernel 2.6.x local root vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-02/0305.html>

From: Frank Louwers (frank_at_openminds.be)

Date: 02/10/04

Date: Tue, 10 Feb 2004 08:42:29 +0100

To: bugtraq@securityfocus.com

On Mon, Feb 09, 2004 at 02:03:47PM -0800, Seth Arnold wrote:

> On Mon, Feb 09, 2004 at 10:23:03PM +0100, Michal Medvecký wrote:

>

> *I haven't got a clue what you're trying to accomplish. If you don't want
> a setuid execute, DON'T RUN chmod +s! You don't even need samba to
> accomplish this:*

>

>

> *I expect this behaviour out of every Linux, BSD, commercial Unix,
> Windows NT with POSIX emulation, QNX, etc.*

>

> *Can you please explain what specifically bothers you?*

I think his point is this:

Image you have a user account luser on box foo. You do not have root on foo. However, you do have root on box bar. If you are allowed to smbmount stuff on foo as user luser, (which is a BadThing(tm), but default behaviour on some systems as it seems), and you smbmount a share on bar, and use that suid shell, you actually have root control on foo!

Kind Regards,
Frank Louwers

--

Openminds bvba www.openminds.be
Tweebruggenstraat 16 - 9000 Gent - Belgium

- application/pgp-signature attachment: [stored](#)