

---

Subject: Re: [linux-cifs-client] oops in khelper  
Posted by [vaverin](#) on Fri, 09 Nov 2007 12:31:12 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Jeff Layton wrote:

> On Fri, 09 Nov 2007 14:17:38 +0300

> Vasily Averin <[vvvs@sw.ru](mailto:vvvs@sw.ru)> wrote:

>  
>> Hello Steve,  
>>  
>> Could you please take a look at the following oops? It looks like it  
>> is related to cifs:  
>> 1) Code line is corrupted (21 byte?!?), It looks like part of CIFS  
>> smb\_hdr with CIFS magic:  
>> 00 00 50 ff 53 4d 42 32 00 00 00 00 80 41 c0 <00> 00 00 00 00 00  
>> FF S M B  
>  
> Looks like the random memory corruption I was chasing around a month  
> ago. It's a nasty bug. This patch from the cifs-2.6 git tree will  
> probably fix it:  
>  
> commit c18c732ec6bf372aa959ca6534cbfc32e464defd  
> Author: Steve French <[sfrench@us.ibm.com](mailto:sfrench@us.ibm.com)>  
> Date: Wed Oct 17 18:01:11 2007 +0000  
>  
> [CIFS] fix bad handling of EAGAIN error on kernel\_recvmsg in cifs\_demultiplex\_thread

Jeff,

thank you for this hint.

However I would pay your attention that our kernel is based on RHEL4, and obviously it is vulnerabled too.

thank you,  
Vasily Averin

---