

Re: samba vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-06/3845.html>

From: Lanny Baron (lhb@freebsdsystems.com)

Date: 06/29/01

From: "Lanny Baron" <lhb@freebsdsystems.com>

To: "Ryan Masse" <mail@max-info.net>

Date: Fri, 29 Jun 2001 04:31:20 GMT

Hello Ryan,

I cannot answer that. I am not a part of The FreeBSD Project Inc. But your question is well taken. In fact Ryan, it was your posting that led me to our mirror of Samba (<http://ca.samba.org/samba/samba.html>) to see what the Samba team had pointed out.

What this really shows is, how well the FreeBSD community works. It's just people like you Ryan, and others that keep other people abreast of things.

Regards,

Lanny

Ryan Masse writes:

> *i'm sure we are all aware of the problem.. my original question was how come*

> *this didn't make the freebsd security advisory?*

>

> *Ryan*

>

>> *Hi,*

>> *I am the Canadian mirror for Samba.org and the warning is right on the*

> *main*

>> *page, under NEWS. It's the macro %m and it warns:*

>>

>> *The security hole occurs when a log file option like the following is*

>> *used:*

>>

>> *log file = /var/log/samba/%m.log*

>>

>> *In that case the attacker can use a locally created symbolic link to*

>> *overwrite any file on the system. This requires local access to the*

>> *server.*

>>

>> *If your Samba configuration has something like the following:*

>>

>> *log file = /var/log/samba/%m*

>>

FreeBSD–Security: Re: samba vulnerability

>> *Then the attacker could successfully compromise your server remotely*
>> *as no symbolic link is required. This type of configuration is very*
>> *rare.*
>>
>> *The most commonly used log file configuration containing %m is the*
>> *distributed in the sample configuration file that comes with Samba:*
>>
>> *log file = /var/log/samba/log.%m*
>>
>> *in that case your machine is not vulnerable to this attack unless you*
>> *happen to have a subdirectory in /var/log/samba/ which starts with the*
>> *prefix "log."*
>>
>> *Regards,*
>> *Lanny*
>>
>> *NAKAJI Hiroyuki writes:*
>>
>> >>>>> *In <200106290052.TAA32034@aristotle.tamu.edu>*
>> >>>>> *rasmith@aristotle.tamu.edu (Robin Smith) wrote:*
>> >
>> > *RS> the %m.log exploit, but now I wonder where it was.*
>> >
>> > *<http://lists.samba.org/pipermail/samba-announce/2001-June/000054.html>*
>> >
>> > *Is this what you read?*
>> > *--*
>> > *NAKAJI Hiroyuki*
>> >
>> > *To Unsubscribe: send mail to majordomo@FreeBSD.org*
>> > *with "unsubscribe freebsd-security" in the body of the message*
>>
>>
>>
>> *~~~~~*
>> *Lanny Baron*
>> *servers with the power to Serve*
>> *<http://www.FreeBSDsystems.com>*
>> *1.877.963.1900*
>>
>> *To Unsubscribe: send mail to majordomo@FreeBSD.org*
>> *with "unsubscribe freebsd-security" in the body of the message*
>>
>
>
>
> *To Unsubscribe: send mail to majordomo@FreeBSD.org*
> *with "unsubscribe freebsd-security" in the body of the message*

FreeBSD–Security: Re: samba vulnerability

~~~~~

Lanny Baron  
servers with the power to Serve  
<http://www.FreeBSDsystems.com>  
1.877.963.1900

To Unsubscribe: send mail to [majordomo@FreeBSD.org](mailto:majordomo@FreeBSD.org)  
with "unsubscribe freebsd–security" in the body of the message