

Re: Q: Impact of globbing vulnerability in ftpd

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-04/2589.html>

From: Crist Clark (crist.clark@globalstar.com)

Date: 04/23/01

Date: Mon, 23 Apr 2001 09:56:12 -0700
From: "Crist Clark" <crist.clark@globalstar.com>
To: Dag-Erling Smorgrav <des@ofug.org>

Dag-Erling Smorgrav wrote:

>
> Victor Sudakov <sudakov@sibptus.tomsk.ru> writes:
>> On Mon, Apr 23, 2001 at 12:16:44PM +0200, Dag-Erling Smorgrav wrote:
>>> As far as I understand, it can be exploited only after a user has
>>> logged in, so ftpd is already chrooted
>>> Not necessarily.
>> Anonymous account is always chrooted. I think you have to play
>> with the source to disable this.
>
> The logged-in user is not necessarily anonymous.
>
>>> Run arbitrary code on the target machine, which may perform operations
>>> (such as creating new directories to store warez) which the FTP server
>>> normally doesn't allow the user to perform,
>> How is this possible if ftpd drops root privileges after
>> successful login?
>
> I didn't claim the code would run as root. It would run as the
> logged-in user, or user "ftp" in case of an anonymous login.

The FTP daemon does NOT drop privileges. It changes effective user ID only. (Do a 'ps -axo pid,command,user,ruser | grep ftpd' on a running daemon.)

>> So, if the users already have shell accounts, this security hole
>> does not matter for me, does it?
>
> Probably not. Depends on your anonftp setup.

Privilege escalation is possible whenever an FTP daemon can be fed arbitrary code to execute.

--

Crist J. Clark
crist.clark@globalstar.com
(408) 933-4387

Network Security Engineer
Globalstar, L.P.
FAX: (408) 933-4926

The information contained in this e-mail message is confidential,

FreeBSD-Security: Re: Q: Impact of globbing vulnerability in ftpd

intended only for the use of the individual or entity named above. If the reader of this e-mail is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any review, dissemination, distribution or copying of this communication is strictly prohibited. If you have received this e-mail in error, please contact postmaster@globalstar.com
To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message