WU-FTP YOUR WAY TO ROOT

SHELL ACCESS THROUGH WU-FTP VULNERABILITIES

By Michael Sparks

OVERVIEW

For the last ten years of my information services career, I have been actively involved in trying to do the right thing. These years included building robust computers with cleanly installed operating systems; implement the most current patches, and provide support that delivered the best possible work environment for my customers. Protection from Fat Fingers, Hackers, Crackers, or Freakers was my guide. Now that security is my primary job, instead of a part-time "Oh we should have somebody take care of security administration" position, I actually can take the time to analyze the dark side that I spent my precious moments protecting our company against. I have decided to accomplish this through the discovery of two Wu-ftp exploits. In the next couple of pages, I have mixed my personal commentaries with definitions, names of the Hacks, or exploits, how the exploit occurs, a link to four code examples of the "Site Exec Hack" (be good!), and what you can do to protect your company against them. I found all this through Internet searches, which spoke directly to these two specific exploits. I hope you enjoy the knowledge explained, as much as I did in researching it. Oh, by the way, I am dying to set up an isolated network at home to try these. Onward!

THE APPLICATION

Wuarchive-ftpd, more affectionately known as wu-ftpd, is a replacement ftp daemon for Unix systems developed at Washington University (*.wustl.edu) by Bryan D. O'Connor. (WHO IS NO LONGER WORKING ON IT OR SUPPORTING IT!) Wu-ftpd is the most popular ftp daemon on the Internet, used on many anonymous ftp sites all around the world.[i] It is a coupled with many well-known systems like Caldera OpenLinux, Conectiva Linux, Debian Linux, HP HP-UX, and RedHat Linux just to name a few. The "Site Exec" exploit is the most referred to when querying the "Web". The "setproctitle" exploit version effects BSD and NetBSD. Currently, you can find the singular application for download, any current updates, and related information at http://www.wu-ftp.org.

THE HACKS

By using Internet search engines from www.excite.com, www.yahoo.com, www.altavista.com, and www.search.com, I was able to find the following two Wu-ftp hacks, or vulnerabilities, that when applied allowed root access:

1) **"Remote format string stack overwrite" or "Site exec" vulnerability**[ii]

2) **"Ftpd setproctitle" vulnerability**[iii]

HOW HACK ONE IS USED

"Remote format string stack overwrite" or "Site exec" vulnerability

Here Wu-ftp is subject to a very serious remote attack using the "Site Exec" command. Input is fed directly into a format string for a *printf function. When this happens it is possible to overwrite important data, such as a return address, on the stack. When this is accomplished, the function can jump into shellcode pointed to by the overwritten Execute Interface Program, or "EIP", and execute arbitrary commands as root. At first analysis, this appears to look like a buffer overflow; it is actually an input validation problem. Just goes to show you that good coding from the start is a valuable practice. Had the original programmer checked for invalid input, I would not be writing this now! Anonymous ftp is exploitable making it even more serious as attacks can come anonymously from anywhere on the Internet. A good time to plug the restriction of Anonymous user for those security people that didn't know or think that this was a good idea already! This code is easily accessible on the Internet and ready to compile. Can you imagine? There were four "C" source code programs available where I derived the majority of this overview. Personally, I like the fourth "C" program as I felt the coder used the best comments and structure. I have included a link to the programs with the caveat that "it is not the bullet that kills the person, but the culprit that pulled the trigger", let your conscience be your guide!

THE CODE

You may view the code at http://www.securityfocus.com/bid/1387 by clicking on the exploit tab, saving the code, and then opening it in a "C" program editor.

HOW HACK TWO IS USED

"Ftpd setproctitle" vulnerability

An improper use of the setproctitle() library function by the "ftpd" daemon may allow a malicious remote ftp client to subvert an FTP server. When this improper use is performed, remote system access is possible.

The BSD setproctitle() function, like printf(), accepts a format string and a variable number of arguments; the format string is interpreted to determine how to display the other arguments to the function. If the format string can contain arbitrary user-supplied data, it may be possible to trick the program into reading or writing arbitrary memory locations, resulting in a security compromise. A more extensive audit of the NetBSD sources for problems of this form is under way.

It has been rumored that this exploit might be used in conjunction with the "Site Exec" exploit. There were no reported incidents confirming this during my research other than a statement in the Cert advisory that I have footnoted. This problem effects all versions of NetBSD.

Syslog entries similar to the following may indicate an attack:[iv]

```
Jul 4 17:43:25 victim ftpd[3408]: USER ftp

Jul 4 17:43:25 victim ftpd[3408]: PASS [malicious shellcode]
Jul 4 17:43:26 victim ftpd[3408]: ANONYMOUS FTP LOGIN FROM
attacker.example.com [10.29.23.19], [malicious shellcode]
Jul 4 17:43:28 victim-site ftpd[3408]: SITE EXEC (lines: 0):
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%
.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%
.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%c%c%c%.f|%p
Jul 4 17:43:28 victim ftpd[3408]: FTP session closed[v]
```

SOLUTIONS

Each of the links that I have cited offer recommended solutions. It is this author's opinion that a due care, or diligence, approach will head off most chances of exploit. This includes upgrading to the newest recommended level of Wu-ftp, installing the current security patches, or disabling FTP services. A good administrator or security manager will include a consistent methodology that reviews, tests, and applies appropriate solutions to his or her production environment.

THOUGHTS

On closing, I just wanted to make some comments regarding exploits. Try to subscribe to a couple of security alert digests so that you are alerted to new exploits and try to keep up on bugs that effect your systems (CERT[vi], SANS[vii], and Security Focus[viii] are a few good security sites with digests) and visit your operating system's site for current information regarding your specific system. As for the research, it was fun and I have viewed many "Security Alerts" as a result. All the while, I have never quite understood this mentality associated with malicious intent. It is one thing to find bugs or improper code. It is another to use this to cause damage to an environment other than your own. If there is a conscience in would be hackers, or whatever term denotes a person that with intent interrupts or denies service of a site other than their own, I implore you to think as most of us who want to do the right thing have heard in our life - "Treat others as you would like to be treated" And most of all, if you think you have put everything into place to secure your environment, please read the boxed quote from one of my favorite childhood books below. Thanks, MJS.

> *"Nothing is impossible, some things are just harder to believe than others" – Euclid Bullfinch*[ix]

[i] van den Hout. Koos. "Frequently Asked Questions about wu-ftpd, with answers" 23 Oct. 2000. URL: http://www.wu-ftpd.org/wu-ftpd-faq.html#QA3

[ii] First posted to Bugtraq by tf8 <tf8@zolo.freelsd.net>. "Wu-Ftpd Remote Format String Stack Overwrite Vulnerability". 22 June 2000. URL: http://www.securityfocus.com/bid/1387

[iii] Jun-ichiro Hagino <itojun@netbsd.org>. "ftpd setproctitle vulnerability". 8 July 2000. URL: http://www.linuxsecurity.com/advisories/netbsd_advisory-545.html

[iv] CERT per Carnegie Mellon. "ftpd vulnerabilities". 2000. URL: http://www.cert.org/present/cert-overview-trends/tsld150.htm

[v] Carnegie Mellon. "CERT® Advisory CA-2000-13 Two Input Validation Problems In FTPD". 21 November 2000. http://www.cert.org/advisories/CA-2000-13.html

[vi] http://www.cert.org

[vii] http://www.sans.org/newlook/home.htm

[viii] http://www.securityfocus.com Click on Bugtraq sidebar link.

[ix] Jay Williams and Raymond Abrashkin. "Danny Dunn and the Anti-Gravity Paint". 1957