

## Re: ISSalert: ISS Security Alert: WU-FTPD Heap Corruption Vulnerability (fwd)

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-12/6975.html>

---

**From:** Przemyslaw Frasunek ([venclin@freebsd.lublin.pl](mailto:venclin@freebsd.lublin.pl))

**Date:** 12/01/01

From: Przemyslaw Frasunek <[venclin@freebsd.lublin.pl](mailto:venclin@freebsd.lublin.pl)>  
To: Konrad Heuer <[kheuer@gwdug60.gwdg.de](mailto:kheuer@gwdug60.gwdg.de)>, [freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org)  
Date: Sat, 1 Dec 2001 12:25:44 +0100

On Friday 30 November 2001 09:53, Konrad Heuer wrote:

> *Any opinions whether wu-ftp on FreeBSD is vulnerable too? To my mind, it*  
> *seems so.*

actually, wu-ftp on FreeBSD is vulnerable, but phk-malloc design prevents from exploiting this. typical scenario of exploitation on linux box is:

– attacker populates heap with pointers to proctitle buf by calling few times 'STAT ~{ptrptrptrptr}'

– after that, attacker does 'STAT {~}' which calls two times blockfree() in ftpglob() and malicious 'ptr' is passed to free()

– in proctitle buf there is a fake malloc chunk, pointing to syslog() GOT entry and shellcode, also located in proctitle buf

– free() when trying to deallocate fake chunk overwrites pointer to syslog() function and then segfaults

– segfault sighandler calls syslog() and shellcode is executed

as you can see, exploitation of this vulnerability isn't so simple. after spending long hours with gdb, looks like it's exploitable only on dlmalloc from glibc.

--

\* Fido: 2:480/124 \*\* WWW: <http://www.frasunek.com/> \*\* NIC-HDL: PMF9-RIPE \*  
\* Inet: [przemyslaw@frasunek.com](mailto:przemyslaw@frasunek.com) \*\* PGP: D48684904685DF43EA93AFA13BE170BF \*  
To Unsubscribe: send mail to [majordomo@FreeBSD.org](mailto:majordomo@FreeBSD.org)  
with "unsubscribe freebsd-security" in the body of the message