

remote command execution in 'tattle'

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-06/0057.html>

From: b0iler (b0iler_at_r00thell.org)

Date: 06/07/05

Date: Tue, 7 Jun 2005 11:17:49 +0100 (BST)

To: bugtraq@securityfocus.com

Hello, a recent bugtraq posting by CISSP C.J. Steele contains a vulnerability which will leave a box possibly open for remote command execution. There are many ways to exploit this, but I chose logging in through ftp with username like

```
sshd rhost 9 10 11 |rm${IFS}-rf${IFS}/|echo'1.1.1.1'
```

because of poor input validation and improper use of system calls in tattle this will execute the `rm -rf /` and `echo'1.1.1.1'` commands. I would assume that in many cases tattle would be running as root. The problem is in the `getemails` subroutine on the line `my $whois = `/usr/bin/whois $tld`;`

Author not notified. I believe he reads this list.

Suggested workaround. Disable tattle until patch.