SPAM attack through vulnerable PHP script

Stefan Hornburg (Racke)

2007-06-15

One of my customers reported this morning that their webserver was unusually slow. I discovered that it was abused for sending SPAM through web forms. The PHP script processing these forms lacked proper input sanitization. After disabling the script by renaming its mail function I deleted almost 1000 of SPAM emails from the queue:

```
xxx:/var/spool/exim4/input# grep -l "Email von yyy.zz:" *-D | perl -pe 's/-D$//' | xargs exim -Mrm
```

Linuxia Wiki

Stefan Hornburg (Racke)
SPAM attack through vulnerable PHP script
2007-06-15

wiki.linuxia.de