

La spirale infernale

Romain Raboin, Raphaël Rigo, Julien Tinnès

France Telecom R&D



La spirale infernale





La source du mal

Diff for /openssl/trunk/rand/md_rand.c between version 140 and 141

version 140, Tue May 2 16:25:19 2006 UTC

version 141, Tue May 2 16:34:53 2006 UTC

271

Line 271

```
else
    MD_Update(&m,&(state[st_idx]),j);
```

```
else
    MD_Update(&m,&(state[st_idx]),j);
```

```
MD_Update(&m,buf,j);
```

```
/*
 * Don't add uninitialised data.
```

```
MD_Update(&m,buf,j);
```

```
*/
```

```
MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
MD_Final(&m,local_md);
md_c[1]++;
```

```
MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
MD_Final(&m,local_md);
md_c[1]++;
```

465

Line 468

```
MD_Update(&m,local_md,MD_DIGEST_LENGTH);
MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
PURIFY
```

```
MD_Update(&m,local_md,MD_DIGEST_LENGTH);
MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
```

```
#ifndef PURIFY
```

```
/*
 * Don't add uninitialised data.
```

```
MD_Update(&m,buf,j); /* purify complains */
```

```
MD_Update(&m,buf,j); /* purify complains */
```

```
*/
```

```
#endif
```

```
k=(st_idx+MD_DIGEST_LENGTH/2)-st_num;
if (k > 0)
```

```
k=(st_idx+MD_DIGEST_LENGTH/2)-st_num;
if (k > 0)
```



Conséquences

- Faille remote (authentification par clé publique)
- Possibilité de déchiffrement des sessions SSH et SSL vers ou depuis une debian - **Y compris avec PFS**
- Cassage de toutes les clés DSAs utilisées sur une Debian



Conséquences (2)

- Logiciels touchés: OpenSSH, OpenVPN, browsers web, serveurs web . . .
- Sans doute la vulnérabilité la plus importante que nous ayons rencontrée
- ?????
- Profit !



Nos outils relatifs à SSH

- Brute-force en remote des clés autorisées (.ssh/authorized_keys) faibles
 - ▶ Écrit en C multithreadé, environ 100 clés/s
 - ▶ Espace des clés couvert en 5 minutes
- Cassage de clés de sessions SSH (Diffie-Hellman)
 - ▶ Si le serveur était vulnérable au moment de la communication
 - ▶ Si le client était vulnérable au moment de la communication
 - ▶ En une minute maximum sur une machine récente

Questions ?



- Cf. <http://cr0.org/progs/sshfun> (peut-être)
- Qui a gardé des pcap de SSTIC 2007 ?

