



Ajankohtaista *X - tietoturvasta
FUUG@Sea 15.9.2000

Riku Kalinen

Guru, CISSP

<riku.kalinen@nixu.fi>

nixu

Nixu Oy
PL 21
(Mäkelinkatu 91)
00601 Helsinki, Finland
tel. +358 9 478 1011
fax. +358 9 478 1030
Ly tunnus: 0721811-7
Kaupparek. 440.982
info@nixu.fi
<http://www.nixu.fi>



Contents

- Nixu Oy
- Selection Criteria
- libc locale problem
- rpc.statd problem (CA-2000-17)
- ftpd problem (CA-2000-13)
- DNS problems (CA-2000-03, CA-99-14)
- Scans and probes
- Conclusion
- Additional information

15.9.2000

n i x u



Nixu Oy

- Internet Solutions
 - Most Valued Partner in Mobile and Secure Internet Infrastructure
 - Independent player
- **Network Security**
- Internet Service Platforms
- Mobile Internet Platforms
- Heavy UNIX and IP Experience

15.9.2000

nixu



Nixu Oy ...

- References (some)
 - SSH IPsec implementation 1997
 - Saudi Arabian Internet implementation 1998 -
- Personnel
 - This week 74
 - The personnel of Nixu is highly educated and many have strong practical experience
 - Many long-term UNIX and IP gurus/wizards
 - Offices in Helsinki, Oulu, Riyadh, Hong Kong

15.9.2000

nixu



Selection Criteria

- From CERT and Bugtraq
- Most interesting problems from Finnish point of view
 - E.g. excluded Kerberos problems

15.9.2000

NIXU



libc locale problem

- Published 4.9.2000 by CORE SDI
 - On bugtraq, various vendors' web sites
- Local root exploit
 - Unprivileged local users can gain root privileges
 - Under certain conditions, also remotely exploitable
 - Attacker must be able to modify target file system before attack
 - Telnetd or something else must (incorrectly) pass enough environment variables thru

15.9.2000

NIXU



libc locale ...

- Input validation error on many C libraries
 - On internationalisation code (locale)
- On many *X systems
 - Solaris 2.x, 7, 8; Linux; AIX?, HP-UX?, Tru64?, SCO?

15.9.2000

NIXU



libc locale ...

- How to fix
 - Apply a patch
 - This will take time since most *X platforms need a patch
 - Before applying a patch, either live with the problem or turn all SUID bits off
 - Many vendors have released patches
 - Disable vulnerable services (only a partial solution)

15.9.2000

NIXU



rpc.statd problem (CA-2000-17)

- Input Validation Problem
- Local or remote users can execute arbitrary code as rpc.statd owner (typically root)
- User-supplied data to syslog() as a format string
 - This is, of course, asking for trouble
 - NEVER EVER trust user/network data

15.9.2000

NIXU



rpc.statd ...

- Traces of successful attack in syslog

```
Aug XX 17:13:08 victim rpc.statd[410]: SM_MON
request for hostname
containing '/': ^D^D^E^E^F
^F^G^G08049f10
bffff754 000028f8 4d5f4d53 72204e4f 65757165
66207473 6820726f 6e74736f
20656d61 746e6f63 696e6961 2720676e 203a272f
...
1<83>
<88>F'<88>F*<83> <88>F<89>F+,
<89><8D>N<8D>V<80>1<89>@<80>/bin
/sh -c echo 9704 stream tcp
nowait root /bin/sh sh -i >> /etc/inetd.conf;killall
-HUP inetd
```

15.9.2000

NIXU



rpc.statd ...

- How to fix:
 - Apply patch (fair)
 - Or block in firewall (better)
 - UDP should be blocked as completely as possible anyhow
 - Usual exceptions: DNS, NTP
 - Or disable altogether if not needed (best)
 - E.g. on Debian GNU/Linux distribution:

```
mv /sbin/rpc.statd /sbin/rpc.statd.disabled
```

15.9.2000

NIXU



ftpd problem (CA-2000-13)

- Two input validation problems
- wu-ftpd \leq 2.6.0; BSD ftpd 5.51, 5.60; some others
- ftpd appears to be very problematic
 - especially on anonymous ftp installations
 - Be VERY careful when installing anonymous ftp service

15.9.2000

NIXU

- Sample log:

15.9.2000

- How to fix:

- 15.9.2000



DNS problems (CA-2000-03, CA-99-14)

- It appears to me that BIND has taken Sendmail's place as a default problem on *X environment
- No good alternative to BIND
 - Code complex like h.ll
 - Relatively fast development
 - New major features added all the time

15.9.2000

NIXU



DNS ...

- Target acquisition particularly easy
 - Port scanning
 - Existing DNS data
 - Trivial to find target systems with minimal effort
- Vulnerable versions bind < 8.2.2p3
- Breaking into active DNS server enables all kinds of nasty tricks
 - E.g. domain hijacking

15.9.2000

NIXU



DNS ...

- Especially those systems that do not any more act as a DNS servers
 - But have active BIND installation still
 - It is easy to install BIND to some machine “temporarily” and forget it on
 - For historical reasons it may be difficult to disable BIND on some machines

15.9.2000

NIXU



DNS ...

- Traces of successful attack:
 - New directories: /var/named/ADMROCKS, /var/named/O
 - Several types of backdoors/trojans installed: sshd, login, inetd, ...
 - Rootkits to cover tracks
 - DoS tools, scanners, exploits, ...

15.9.2000

NIXU



DNS ...

- How to fix:
 - Patch, block, disable as above
 - Additionally, run chrooted
 - Big hand to OpenBSD team to make BIND start chrooted by default

15.9.2000

NIXU



Scans and probes (CERT 31.8.2000)

- Sadly long list of protocols with known problems
 - TCP: 21, 22, 53, 98, 109, 110, 111, 139, 143, 543, 1080, 5135
 - UDP: 53, 137, 138
 - ICMP: 0, 8
- In addition to these, various known backdoors and trojans are scanned all the time
- You should block all unnecessary traffic
 - Preferably with stateful filters

15.9.2000

NIXU



Conclusion

- Security is a process, not a project
- Disable unnecessary services
- Block unnecessary traffic
- Keep your systems up-to-date
 - Follow relevant sources
 - CERT
 - Bugtraq
 - ...

15.9.2000

NIXU



Additional information

- CERT
 - <http://www.cert.org>
 - Very good quality
 - Sometimes late
- Bugtraq mailing list
 - <http://www.securityfocus.com>
 - Also loads of other stuff
 - Fast
 - Poor signal-to-noise ratio

15.9.2000

NIXU



Questions ?