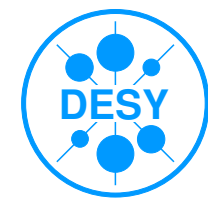




Kernel Issues

- ptrace local root exploit
- npt module
- afs modules
- server kernels
- workstation kernels
- plans



ptrace local root exploit (1)

- local users can gain root privileges trivially
- affects all 2.2.x up to 2.2.24 (2.2.25 is fixed)
- affects all 2.4.x up to 2.4.20
- patches are available for 2.4.18 and higher
- exploit code released to the web around March 18
- started working on new kernels ASAP
- new server kernels available since March 24
- rolled out ptrace blocking module on DL4 on March 28



ptrace local root exploit (2)

- one compromised workstation at DESY (March 24)
- several compromised systems at CERN March 18-30
- incident notices received from many HEP institutes and universities
- we are monitoring DL systems for root kits
- no further incidents observed

<http://www-it.desy.de/systems/linux/desy-4/ptrace-fix.html>



npt module

- simple kernel module to catch ptrace calls
- borrowed hacker code from 2001 to start with
- compiles on both 2.2.x and 2.4.x kernels
- provided makefile and SALAD card
- module compiles itself on target system using installed kernel's include files, inserts itself into running kernel and is loaded on reboot in `/etc/rc.local`
- current version breaks ptrace, breaks gdb
- spent significant time on more elaborate handler, to no avail



afs modules

- current AFS RPM is `afs-aware-2.4.18.17`
- still uses OpenAFS 1.2.3
- AFS servers at DESY are 1.2.8 since December
- every kernel upgrade (and almost any patch) requires new AFS modules
- we had a hard time keeping up recently
- AFS seems to be the most sensitive system component right now
- we know that it is possible to bring down a 2.4.18 kernel by writing to AFS with the `O_SYNC` option on (fetchmail does ...)



server kernels

- current best DESY version is `wgs-kernel-SMP-2.4.18-10.i386.rpm`
- patched against ptrace bug
- we know that 2.4.10 to 2.4.18 can have problems with synchronous writes (caused by new memory manager in 2.4.10), our old 2.4.7 is immune
- 2.4.19 was released last July with lag bug and ext3 data corruption bug
- 2.4.20 still has a data corruption bug in ext3 (rel. Nov 2002)
- Most recent kernel is 2.4.21-pre3-ac4, released Jan 12
- no release date for 2.4.21 set yet
- development work stopped for now



workstation kernels

- current best DESY version is `desktop-kernel-SMP-2.4.18-8.i386.rpm`
- there is a patched `desktop-kernel-SMP-2.4.18-11.i386.rpm` available on request which breaks sound support (need to recompile ALSA modules)
- if you do not use debuggers, there is no need to upgrade
- development work stopped for now

plans



- agree on a next DESY kernel for DL4 (2.4.21?)
- rework kernel build system
- build new OpenAFS 1.2.8 clients
- integrate AFS and ALSA into kernel build and kernel RPM
- release after thorough testing

Is it an option to use SuSE stock kernels?

Would other distributions be easier to handle?