

44CON uncovered



Tim Brown - Head Of Research

Portcullis Computer Security Ltd – www.portcullis-security.com

 [/company/portcullis](https://www.linkedin.com/company/portcullis)

 [@portcullis](https://twitter.com/portcullis)

 [/PortcullisCSL](https://www.facebook.com/PortcullisCSL)

 [gplus.to/portcullis](https://plus.google.com/portcullis)

CONTENT/TOPICS

- What this talk will cover
 - Stuff I couldn't discuss at 44CON

Portcullis Computer Security Ltd – www.portcullis-security.com



WHY THIS IS IMPORTANT

- UNIX is still everywhere
- ... except the Desktop (maybe next year?)
 - Android
 - IOS
 - Your favorite embedded device
 - Your bank

Portcullis Computer Security Ltd – www.portcullis-security.com

THE ATTACK SURFACE

| OS | Kernel | Services | |
|-----------------|------------|------------|------------|
| Enterprise apps | Services | Batch jobs | User roles |
| DevOps | Batch jobs | User roles | |
| Users | Misfortune | Malice | |

Portcullis Computer Security Ltd – www.portcullis-security.com

ANTI-EXPLOIT MITIGATIONS

| Mitigation | * GNU/Linux | Solaris 11 | AIX 7 |
|--|-------------|----------------------------------|--------------------------------|
| Mandatory access control | Y | N (Y with Trusted Extensions) | N (Y in Trusted AIX) |
| Non-executable stack | Y | Y | Y (select mode by default) |
| ASLR | Y | Y (tagged-files mode by default) | N (although there is rebasing) |
| Hardened malloc() | Y | N | N (Y with Watson malloc()) |
| Stack cookies and other compile time mitigations | Y (glibc) | N | N |
| mmap() NULL | N | Y | N |

Portcullis Computer Security Ltd – www.portcullis-security.com

OTHER CONTROLS

- Solaris 11 allows privilege management via either traditional RBAC or sudo - first user gets root equivalence
- AIX 7.1 also has Trusted Execution but it's rarely switched on - it's on the hit list
- Linux has symlink attack mitigations
- Solaris has a hardened runtime linker

FUZZING USB ON AIX

- Used the anykey0x.de
- Intended to emulate various USB devices
 - Tried my own fuzzer
 - `return(ENOBUGS)`
- Turns out that, AIX doesn't support more than basic HID functionality

syscall()

- `int syscall(int number, ...);`
- Kernel provided basic functions (usually)
- Not always kernel land e.g. QNX:
 - Uses `MsgSendnc()` to send to `procmgr`
 - We can send from user land
 - Could be a fun target for fuzzing?

MY 1ST KERNEL BUG

- Consider the following:

```
int randomsyscall(int size, void *value) {  
    if (size > maxsize) size = maxsize;  
    void *a = kmalloc(size);  
    privop(a, size);  
    copytouser(a, value, size);  
    return SUCCESS;  
}
```

- What's wrong?

MY 1ST KERNEL BUG

- Actually affects AIX ptrace() implementation
- Signedness bug, impact DoS or disclosure
- Allows leaks to WPARs from global environment

```
$ id
uid=208(tmb) gid=1(staff)
$ while ;; do ./x | grep "root"; done
...LOGNAME=root...USER=root...PWD=/...
```

Portcullis Computer Security Ltd – www.portcullis-security.com

ioctl()

- `int ioctl(int fildes, int request, ... /* arg */);`
- Intended to allow device driver interaction
 - Tried my own fuzzer
 - Ported Ilja Van Sprundel's fuzzer
 - `return(ENOBUGS)`
- But AIX is terrible? Fuzz deeper, “The type of arg depends upon the particular control request, but it shall be either an integer or a pointer to a device-specific data structure.”

IPC

- UNIX sockets
- Signals
- System V semaphores (sem*)
- System V shared memory (shm*)
- System V messages (msg*)
- POSIX semaphores (sem_*)
- POSIX shared memory (shm_*)
- POSIX messages (mq_*)

socket()

- `int socket(int domain, int type, int protocol);`
- Typically used for establishing TCP and UDP connections
 - There are domains e.g. `AF_UNIX`
- Scan them with `UNIXSocketScan`
 - Utilises `nmap` and custom probes
 - Who knew CUPS supported HTTP over a UNIX socket?
 - Expect a blog post on Windows pipes

signal()

- `void (*signal(int sig, void (*func)(int)))(int);`
- Used to trigger functions on exceptional events
- Fuzz them using SIGnalGenerator
- Which signals?
 - Read the source
 - Make use of gdb/objdump
 - USR1 and USR2 are “undefined” - man -K "USR1" - @climagic

REMEMBER 44CON 2012?

- ftp et al are setuid on AIX
 - Apparently for additional logging
- Problems? Utilises SIGINT
 - Toggles into a privileged state to log
 - What if we trigger a signal whilst it's already in the signal handler (i.e. uid=0)

```
ftp> malloc: Not enough space
```

Portcullis Computer Security Ltd – www.portcullis-security.com

shmget()

- `int shmget(key_t key, size_t size, int shmflg);`
- Patient 0 (CVE-2013-025) spotted by @pentestmonkey
- Insecure permissions on System V Shared Memory
 - Affected Qt and by extension KDE
 - Allows reading and writing

ANALYSING DEBIAN

- Utilised <http://codesearch.debian.net/>
- (Eventually) Coccinelle

Portcullis Computer Security Ltd – www.portcullis-security.com

BUGS FOUND?

- 486 packages using shmget():
 - 89 cases of shmget() being called insecurely, to support X11 protocol (58 packages)
 - 212 other cases of shmget() being called insecurely (114 packages)
 - 80 cases of shmget() being called potentially insecurely, to support X11 (44 packages)
- Similar for semget(), shmctl() and semctl()

Portcullis Computer Security Ltd – www.portcullis-security.com

MEMORY CORRUPTION?

- Write honoured on both AIX and Linux
- Execute honoured on neither AIX or Linux
 - Always executable on AIX, never on Linux
- ASLR on Linux when `randomize_va_space` ≥ 1
 - Breaks IBM DB2

REMEDIATION

- Qt (CVE-2013-0254) and Java JRE (CVE-2013-1500) patched
- I gave up with Red Hat or Debian :(
- IBM DB2 and IBM WebSeries MQ are affected
 - Doubtless more to find, iSeries supports shmget() and I've seen similar problems there :P
- Achievement unlocked, @grsecurity patch released

Portcullis Computer Security Ltd – www.portcullis-security.com

shm_open()

- `int shm_open(const char *name, int oflag, mode_t mode);`
- In theory, allows privilege escalation – more interesting than System V Shared Memory
 - Not on AIX though :P

IN PRACTICE ^ Wfglrx-driver

```
17c3ae0:  ba b6 01 00 00      mov  $0x1b6,%edx; mode = 0666
17c3ae5:  be 42 00 00 00      mov  $0x42,%esi; oflag = O_CREAT | O_RDWR - missing O_EXCL
17c3aea:  4c 89 ef            mov  %r13,%rdi
17c3aed:  e8 76 50 a4 fe      callq 208b68 <shm_open@plt>
17c3af2:  45 31 e4            xor  %r12d,%r12d
17c3af5:  83 f8 ff            cmp  $0xffffffff,%eax
17c3af8:  89 c5                mov  %eax,%ebp
17c3afa:  74 c1                je   17c3abd
<pthread_attr_setdetachstate@plt+0x15ba3b5>
17c3afc:  be b6 01 00 00      mov  $0x1b6,%esi; mode = 0666
17c3b01:  89 c7                mov  %eax,%edi
17c3b03:  e8 50 55 a4 fe      callq 209058 <fchmod@plt>
17c3b08:  48 89 de            mov  %rbx,%rsi
17c3b0b:  89 ef                mov  %ebp,%edi
17c3b0d:  e8 56 59 a4 fe      callq 209468 <ftruncate@plt>
```

Portcullis Computer Security Ltd – www.portcullis-security.com



!POSIX

- On Linux, `fs.protected_symlinks = 1` mitigates exposure
- AIX doesn't even expose `shm_open()` at the file system level

BREAKING THE LINKS

- There's an easy privilege escalation bug in all versions of AIX
 - Fixed as CVE-2012-2179/CVE-2014-3977 - thanks MITRE!

Portcullis Computer Security Ltd – www.portcullis-security.com



WHY 2 CVEs?

- Original bug was trusting ODMERR when setuid binaries are executed
- Initial fix was to check if ODMTRACE0 exists
- So what happens if the symlink is created after this check but before the file is opened?
- Half expecting IBM to make the same mistake with the runtime linker bug fix

ARBITRARY WRITES

- Locate something useful
 - /lib is good if setuid binaries load from /usr/lib
 - Write a new library with a malicious _ctor

EXPLOITING THE LINKER

- RPATH situation worse than first imagined, especially setuid XCOFF binaries
- We have privilege escalation bugs out with at least 4 vendors covering 8 high end products
 - Multiple IBM products (CVE-2014-0907), BMC Patrol (CVE-2014-2591) and multiple HP products (CVE-2013-6216) have already been published
- HP were really good! BMC not so...

!EXPLOITABLE

- Exploitation on Solaris not possible due to hardened runtime linker
 - Relative RPATHs untrusted when setuid binaries executed

WHAT ABOUT PATH?

- Another good target for privilege escalation
 - Generalising the vulnerability class
 - How we identified the ibstat vulnerability from a patch

PATH MISDIRECTION

- Strings the setuid binary taking first word from each line
 - Does it start with /?
 - Any sign of [\\|>|<|;|&]?
 - Parse and repeat
 - Does which \$word yield a match
 - We have a winner!
- Automated in unix-privesc-check 2
- 5 minutes to find an SAP bug \\o/

UNPACKING PATCHES

- .epkgs are just tarballs
- Unsigned, funny considering SUMA
- Contains a manifest called eclist
- Diff the binaries to locate the bugs

Portcullis Computer Security Ltd – www.portcullis-security.com

ABOUT SUMA

- “The technology offered by SUMA assists in moving clients toward an autonomic maintenance strategy by automating the download of software maintenance updates, which allows clients to take advantage of the increased security and reliability benefits of having current fixes, and the cost benefits which result from spending less time on system administration.”
- Not seen in the wild, probably a good thing...
- HTTP → FTP

Portcullis Computer Security Ltd – www.portcullis-security.com

WHERE NEXT?

- Better hardening
 - Using existing mitigations
 - Kernel/runtime linker patches
 - Developing UNIX SDL
- Automated bug hunting
 - Bringing unix-privesc-check 2 on stream
- Migration to other OS?

WANT TO KNOW MORE?

- Come talk to me
- I'm not going to spill all of the beans
- ... but these sessions are about meant to be about sharing what works and what doesn't!
- Build reviews shouldn't just be policy exercises
- ... and there are still ftpd, SunRPC bugs to be crushed!

Portcullis Computer Security Ltd – www.portcullis-security.com




fclose(presentation)



Twitter: @portcullislabs

Web: <http://labs.portcullis.co.uk/>

Portcullis Computer Security Ltd – www.portcullis-security.com

 /company/portcullis

 @portcullis

 /PortcullisCSL

 gplus.to/portcullis