|  |
| --- |
| { |
|  | "defaultAction": "SCMP\_ACT\_ERRNO", |
|  | "archMap": [ |
|  | { |
|  | "architecture": "SCMP\_ARCH\_X86\_64", |
|  | "subArchitectures": [ |
|  | "SCMP\_ARCH\_X86", |
|  | "SCMP\_ARCH\_X32" |
|  | ] |
|  | }, |
|  | { |
|  | "architecture": "SCMP\_ARCH\_AARCH64", |
|  | "subArchitectures": [ |
|  | "SCMP\_ARCH\_ARM" |
|  | ] |
|  | }, |
|  | { |
|  | "architecture": "SCMP\_ARCH\_MIPS64", |
|  | "subArchitectures": [ |
|  | "SCMP\_ARCH\_MIPS", |
|  | "SCMP\_ARCH\_MIPS64N32" |
|  | ] |
|  | }, |
|  | { |
|  | "architecture": "SCMP\_ARCH\_MIPS64N32", |
|  | "subArchitectures": [ |
|  | "SCMP\_ARCH\_MIPS", |
|  | "SCMP\_ARCH\_MIPS64" |
|  | ] |
|  | }, |
|  | { |
|  | "architecture": "SCMP\_ARCH\_MIPSEL64", |
|  | "subArchitectures": [ |
|  | "SCMP\_ARCH\_MIPSEL", |
|  | "SCMP\_ARCH\_MIPSEL64N32" |
|  | ] |
|  | }, |
|  | { |
|  | "architecture": "SCMP\_ARCH\_MIPSEL64N32", |
|  | "subArchitectures": [ |
|  | "SCMP\_ARCH\_MIPSEL", |
|  | "SCMP\_ARCH\_MIPSEL64" |
|  | ] |
|  | }, |
|  | { |
|  | "architecture": "SCMP\_ARCH\_S390X", |
|  | "subArchitectures": [ |
|  | "SCMP\_ARCH\_S390" |
|  | ] |
|  | } |
|  | ], |
|  | "syscalls": [ |
|  | { |
|  | |  | | --- | | "names": [ | |  | | |  | | --- | | "accept4", | | "access", | | "alarm", | | "alarm", | | "bind", | | "brk", | | "capget", | | "capset", | | "chdir", | | "chmod", | | "chown", | | "chown32", | | "close", | | "connect", | | "copy\_file\_range", | | "creat", | | "dup", | | "dup2", | | "dup3", | | "epoll\_create", | | "epoll\_create1", | | "epoll\_ctl", | | "epoll\_ctl\_old", | | "epoll\_pwait", | | "epoll\_wait", | | "epoll\_wait\_old", | | "eventfd", | | "eventfd2", | | "execve", | | "execveat", | | "exit", | | "exit\_group", | | "faccessat", | | "fadvise64", | | "fadvise64\_64", | | "fallocate", | | "fanotify\_mark", | | "fchdir", | | "fchmod", | | "fchmodat", | | "fchown", | | "fchown32", | | "fchownat", | | "fcntl", | | "fcntl64", | | "fdatasync", | | "fgetxattr", | | "flistxattr", | | "flock", | | "fork", | | "fremovexattr", | | "fsetxattr", | | "fstat", | | "fstat64", | | "fstatat64", | | "fstatfs", | | "fstatfs64", | | "fsync", | | "ftruncate", | | "ftruncate64", | | "futex", | | "futimesat", | | "getdents", | | "getdents64", | | "getpeername", | | "getpgid", | | "getpgrp", | | "getpid", | | "getppid", | | "getpriority", | | "getresgid", | | "getresgid32", | | "getresuid", | | "getresuid32", | | "get\_robust\_list", | | "getsockname", | | "getsockopt", | | "get\_thread\_area", | | "gettid", | | "inotify\_add\_watch", | | "inotify\_init", | | "inotify\_init1", | | "inotify\_rm\_watch", | | "io\_cancel", | | "ioctl", | | "io\_destroy", | | "io\_getevents", | | "ioprio\_get", | | "ioprio\_set", | | "io\_setup", | | "io\_submit", | | "ipc", | | "kill", | | "lchown", | | "lchown32", | | "lgetxattr", | | "link", | | "linkat", | | "listen", | | "listxattr", | | "llistxattr", | | "\_llseek", | | "lremovexattr", | | "lseek", | | "lsetxattr", | | "lstat", | | "lstat64", | | "madvise", | | "memfd\_create", | | "mincore", | | "mkdir", | | "mkdirat", | | "mknod", | | "mknodat", | | "mlock", | | "mlock2", | | "mlockall", | | "mmap", | | "mmap2", | | "mprotect", | | "mq\_getsetattr", | | "mq\_notify", | | "mq\_open", | | "mq\_timedreceive", | | "mq\_timedsend", | | "mq\_unlink", | | "mremap", | | "msgctl", | | "msgget", | | "msgrcv", | | "msgsnd", | | "msync", | | "munlock", | | "munlockall", | | "munmap", | | "newfstatat", | | "\_newselect", | | "open", | | "openat", | | "pause", | | "pipe", | | "pipe2", | | "poll", | | "ppoll", | | "prctl", | | "pread64", | | "preadv", | | "prlimit64", | | "pselect6", | | "pwrite64", | | "pwritev", | | "read", | | "readahead", | | "readlink", | | "readlinkat", | | "readv", | | "recv", | | "recvfrom", | | "recvmmsg", | | "recvmsg", | | "remap\_file\_pages", | | "removexattr", | | "rename", | | "renameat", | | "renameat2", | | "restart\_syscall", | | "rmdir", | | "rt\_sigaction", | | "rt\_sigpending", | | "rt\_sigprocmask", | | "rt\_sigqueueinfo", | | "rt\_sigreturn", | | "rt\_sigsuspend", | | "rt\_sigtimedwait", | | "rt\_tgsigqueueinfo", | | "sched\_getaffinity", | | "sched\_getattr", | | "sched\_getparam", | | "sched\_get\_priority\_max", | | "sched\_get\_priority\_min", | | "sched\_getscheduler", | | "sched\_rr\_get\_interval", | | "sched\_setaffinity", | | "sched\_setattr", | | "sched\_setparam", | | "sched\_setscheduler", | | "sched\_yield", | | "seccomp", | | "select", | | "semctl", | | "semget", | | "semop", | | "semtimedop", | | "send", | | "sendfile", | | "sendfile64", | | "sendmmsg", | | "sendmsg", | | "sendto", | | "setitimer", | | "setpgid", | | "setpriority", | | "set\_robust\_list", | | "setsockopt", | | "set\_thread\_area", | | "set\_tid\_address", | | "shmat", | | "shmctl", | | "shmdt", | | "shmget", | | "shutdown", | | "sigaltstack", | | "signalfd", | | "signalfd4", | | "sigreturn", | | "socket", | | "socketcall", | | "socketpair", | | "splice", | | "stat", | | "stat64", | | "statfs", | | "statfs64", | | "symlink", | | "symlinkat", | | "sync", | | "sync\_file\_range", | | "syncfs", | | "sysinfo", | | "syslog", | | "tee", | | "tgkill", | | "tkill", | | "truncate", | | "truncate64", | | "ugetrlimit", | | "umask", | | "uname", | | "unlink", | | "unlinkat", | | "utime", | | "utimensat", | | "utimes", | | "vfork", | | "vmsplice", | | "wait4", | | "waitid", | | "waitpid", | | "write", | | "writev" | |   "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": {}, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "personality" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [ |
|  | { |
|  | "index": 0, |
|  | "value": 0, |
|  | "valueTwo": 0, |
|  | "op": "SCMP\_CMP\_EQ" |
|  | } |
|  | ], |
|  | "comment": "", |
|  | "includes": {}, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "personality" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [ |
|  | { |
|  | "index": 0, |
|  | "value": 8, |
|  | "valueTwo": 0, |
|  | "op": "SCMP\_CMP\_EQ" |
|  | } |
|  | ], |
|  | "comment": "", |
|  | "includes": {}, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "personality" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [ |
|  | { |
|  | "index": 0, |
|  | "value": 4294967295, |
|  | "valueTwo": 0, |
|  | "op": "SCMP\_CMP\_EQ" |
|  | } |
|  | ], |
|  | "comment": "", |
|  | "includes": {}, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "breakpoint", |
|  | "cacheflush", |
|  | "set\_tls" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "arches": [ |
|  | "arm", |
|  | "arm64" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "arch\_prctl" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "arches": [ |
|  | "amd64", |
|  | "x32" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "modify\_ldt" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "arches": [ |
|  | "amd64", |
|  | "x32", |
|  | "x86" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "s390\_pci\_mmio\_read", |
|  | "s390\_pci\_mmio\_write", |
|  | "s390\_runtime\_instr" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "arches": [ |
|  | "s390", |
|  | "s390x" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "open\_by\_handle\_at" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_DAC\_READ\_SEARCH" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "bpf", |
|  | "clone", |
|  | "fanotify\_init", |
|  | "lookup\_dcookie", |
|  | "mount", |
|  | "name\_to\_handle\_at", |
|  | "perf\_event\_open", |
|  | "setdomainname", |
|  | "sethostname", |
|  | "setns", |
|  | "umount", |
|  | "umount2", |
|  | "unshare" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_ADMIN" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "clone" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [ |
|  | { |
|  | "index": 0, |
|  | "value": 2080505856, |
|  | "valueTwo": 0, |
|  | "op": "SCMP\_CMP\_MASKED\_EQ" |
|  | } |
|  | ], |
|  | "comment": "", |
|  | "includes": {}, |
|  | "excludes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_ADMIN" |
|  | ], |
|  | "arches": [ |
|  | "s390", |
|  | "s390x" |
|  | ] |
|  | } |
|  | }, |
|  | { |
|  | "names": [ |
|  | "clone" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [ |
|  | { |
|  | "index": 1, |
|  | "value": 2080505856, |
|  | "valueTwo": 0, |
|  | "op": "SCMP\_CMP\_MASKED\_EQ" |
|  | } |
|  | ], |
|  | "comment": "s390 parameter ordering for clone is different", |
|  | "includes": { |
|  | "arches": [ |
|  | "s390", |
|  | "s390x" |
|  | ] |
|  | }, |
|  | "excludes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_ADMIN" |
|  | ] |
|  | } |
|  | }, |
|  | { |
|  | "names": [ |
|  | "reboot" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_BOOT" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "chroot" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_CHROOT" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "delete\_module", |
|  | "init\_module", |
|  | "finit\_module", |
|  | "query\_module" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_MODULE" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "acct" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_PACCT" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "kcmp", |
|  | "process\_vm\_readv", |
|  | "process\_vm\_writev", |
|  | "ptrace" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_PTRACE" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "iopl", |
|  | "ioperm" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_RAWIO" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "settimeofday", |
|  | "stime", |
|  | "adjtimex" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_TIME" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | }, |
|  | { |
|  | "names": [ |
|  | "vhangup" |
|  | ], |
|  | "action": "SCMP\_ACT\_ALLOW", |
|  | "args": [], |
|  | "comment": "", |
|  | "includes": { |
|  | "caps": [ |
|  | "CAP\_SYS\_TTY\_CONFIG" |
|  | ] |
|  | }, |
|  | "excludes": {} |
|  | } |
|  | ] |
|  | } |