

NAME

getentropy - get entropy

LIBRARY

Standard C Library (libc, -lc)

SYNOPSIS

```
#include <unistd.h>
```

int

```
getentropy(void *buf, size_t buflen);
```

DESCRIPTION

getentropy() fills a buffer with high-quality random data.

The maximum *buflen* permitted is 256 bytes.

If it does not produce an error, **getentropy()** always provides the requested number of bytes of random data.

Similar to reading from */dev/urandom* just after boot, **getentropy()** may block until the system has collected enough entropy to seed the CSPRNG.

IMPLEMENTATION NOTES

The **getentropy()** function is implemented using `getrandom(2)`.

RETURN VALUES

Upon successful completion, the value 0 is returned; otherwise the value -1 is returned and the global variable *errno* is set to indicate the error.

ERRORS

getentropy() will succeed unless:

[EFAULT] The *buf* parameter points to an invalid address.

[EIO] Too many bytes requested, or some other fatal error occurred.

SEE ALSO

`getrandom(2)`, `arc4random(3)`, `random(4)`

STANDARDS

getentropy() is non-standard. It is present on OpenBSD and Linux.

HISTORY

The **getentropy()** function appeared in OpenBSD 5.6. The FreeBSD libc compatibility shim first appeared in FreeBSD 12.0.