# CVE-2020-10933: Heap exposure vulnerability in the socket library

Posted by mame on 31 Mar 2020

A heap exposure vulnerability was discovered in the socket library. This vulnerability has been assigned the CVE identifier CVE-2020-10933. We strongly recommend upgrading Ruby.

## Details

When `BasicSocket#recv_nonblock` and `BasicSocket#read_nonblock` are invoked with size and buffer arguments, they initially resize the buffer to the specified size. In cases where the operation would block, they return without copying any data. Thus, the buffer string will now include arbitrary data from the heap. This may expose possibly sensitive data from the interpreter.

This issue is exploitable only on Linux. This issue had been since Ruby 2.5.0; 2.4 series is not vulnerable.

## Affected versions

- Ruby 2.5 series: 2.5.7 and earlier
- Ruby 2.6 series: 2.6.5 and earlier
- Ruby 2.7 series: 2.7.0
- prior to master revision 61b7f86248bd121be2e83768be71ef289e8e5b90

## Credits

Thanks to Samuel Williams for discovering this issue.

## History

- Originally published at 2020-03-31 12:00:00 (UTC)

**Recent News**

Ruby 3.2.0 RC 1 Released
Ruby 3.1.3 Released
Ruby 3.0.5 Released
Ruby 2.7.7 Released
CVE-2021-33621: HTTP response splitting in CGI

Syndicate

Recent News (RSS)