

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

List: [ncurses-bug](#)
Subject: [Re: SPAM: \[security\]\[ncurses\] infocmp -i stack buffer overflow \(CVE-121\), request CVE](#)
From: [Thomas Dickey <dickey@invisible-island.net>](#)
Date: [2025-12-10 20:00:21](#)
Message-ID: [aTnRVcnSSQW79rgq_\(\)_pr1-debianold-64 ! jexium-island ! net](#)
[\[Download RAW message or body\]](#)

On Wed, Dec 10, 2025 at 10:40:49PM +0800, Yixuan Cao wrote:

> Hi Thomas and ncurses maintainers,
>
>
> I am reporting a stack buffer overflow in ncurses (infocmp -i /
> analyze_string). This is a private, responsible disclosure. Please advise
> your preferred coordination timeline.

this is a publicly-viewable mailing list

> Summary
> - Affected component: progs/infocmp.c, function analyze_string()
> - Issue: copies unbounded CSI parameter substrings into 4096-byte stack buffers \
> (buf2/buf3). On glibc builds _nc_STRNCPY falls back to strcpy, so a long SGR \
> parameter list overflows buf2.
> - Impact: Local attacker controlling a terminfo entry can cause denial of service \
> and potentially gain code execution under the privileges of the user running \
> infocmp. The attack surface is any terminfo path accessible to the attacker (e.g., \
> \$HOME/.terminfo or TERMINFO).
>
> Affected version
> - Reproduced on ncurses 6.4 (official tarball from \
> <https://invisible-mirror.net/archives/ncurses/ncurses-6.4.tar.gz>). Please confirm \
> other versions/branches.

that's old (I'll check to see what might apply to 6.5)

--
Thomas E. Dickey <dickey@invisible-island.net>
<https://invisible-island.net>

[\["signature.asc" \(application/pgp-signature\)\]](#)

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

[Configure](#) | [About](#) | [News](#) | [Add a list](#) | Sponsored by [KoreLogic](#)