☆ Starred by 2 users

Owner:	taviso@google.com
CC:	proje...@google.com
Status:	Fixed *(Closed)*
Components:	----
Modified:	Oct 26, 2021

Deadline-90
Finder-taviso
CCProjectZeroMembers
Vendor-Vandyke
Product-securecrt
Reported-2020-Apr-27
Fixed-2020-May-14

Issue 2033: securecrt: memory corruption in CSI functions CVE-2020-12651

Reported by taviso@google.com on Mon, Apr 27, 2020, 5:59 PM EDT Project Member

Code 1 of 13 Back to list

I noticed a vulnerability in SecureCRT that allows a remote system to corrupt memory in the terminal process and execute arbitrary code.

The bug is that if you specify a line number to CSI functions that exceeds INT_MAX, the unsigned integer is used in signed comparisons and wraps around.

https://invisible-island.net/xterm/ctlseqs/ctlseqs.html#h3-Functions-using-CSI-_-ordered-by-the-final-character_s_

The terminal has an array of line buffers it uses for managing the current screen, and this bug means you can corrupt buffers outside of those array bounds.

To reproduce this bug, follow the following steps:
(I tested VT100 and XTerm emulation on Windows 10 x64, I assume other platforms/configurations are affected).

1. Create a new SSH session, accept all the default settings.
2. Connect to a remote system, and run this command (I assume gnu printf):

```
$ printf "\e[%uM%*c" -$((1 << 30)) $COLUMNS A
```

That's CSI DL (Delete Line), but other line functions work too, e.g. IL, but it requires a longer reproducer:

```
$ tput clear; tput cup 0 0; for ((i=0; i < 32; i++)); do
> printf "\e[%huL%*c\r" $((-i & 0xffffffff)) $COLUMNS A
> done
```

In a real attack this might be an SSH banner or similar.

This bug is subject to a 90 day disclosure deadline. After 90 days elapse, the bug report will become visible to the public. The scheduled disclosure date is 2020-06-27. Disclosure at an earlier date is possible if **agreed upon by all parties.**

Comment 1 by taviso@google.com on Mon, Apr 27, 2020, 6:02 PM EDT Project Member

Labels: -Reported-2020-06-27 Reported-2020-04-27

Comment 2 by taviso@google.com on Mon, May 4, 2020, 3:12 PM EDT Project Member

VanDyke replied:

Our development team has been able to implement a fix to address the issue.

This fix will be available in the upcoming 8.7.2 release we anticipate should be made available some time mid-May.

They also sent me a pre-release build, which did address the bugs I reported.

I asked if they wanted me to assign a CVE for them or not.

Comment 3 by taviso@google.com on Tue, May 5, 2020, 1:51 PM EDT Project Member

I went ahead and assigned CVE-2020-12651.

Comment 4 by taviso@google.com on Tue, May 5, 2020, 1:52 PM EDT Project Member

Summary: securecrt: memory corruption in CSI functions CVE-2020-12651 (was: securecrt: memory corruption in CSI functions)

Comment 5 by taviso@google.com on Thu, May 14, 2020, 12:53 AM EDT Project Member

I think we're looking good for a release tomorrow, we're all agreed, the fixes looks good and everything went really smoothly.

That was fast, everything went well.

The plan is to unrestrict this issue, and VanDyke will have an advisory.

Comment 6 by taviso@google.com on Thu, May 14, 2020, 7:41 PM EDT Project Member

Status: Fixed (was: New)
Labels: -Restrict-View-Commit

This is live now, unrestricting as agreed.

https://www.vandyke.com/products/securecrt/history.txt

Changes in SecureCRT 8.7.2 (Official) -- May 14, 2020

Vulnerabilities addressed:

```
 - When certain emulation functions received a large negative number
   as a parameter, it could have allowed the remote system to corrupt
   memory in the terminal process, potentially causing the execution
   of arbitrary code or a crash.
```

Comment 7 by hawkes@google.com on Mon, Jun 22, 2020, 1:16 PM EDT

Labels: -Reported-2020-04-27 Reported-2020-Apr-27

Comment 8 by rschoen@google.com on Tue, Oct 26, 2021, 6:06 PM EDT Project Member

Labels: Fixed-2020-May-14