security-assessment.com

Vulnerability Advisory

Name	SecureCRT - Remote Command Execution
Vendor Update	http://www.vandyke.com/download/securecrt/index.html
Date Released	November 23, 2004
Affected Software	SecureCRT V4.1, V4.0 (and probably lower)
Researcher	Brett Moore brett.moore@security-assessment.com

Description

We discovered a remotely exploitable command execution vulnerability in secureCRT from Vandyke.com.

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">

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.

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.

Exploitation

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.

Solution

Install the vendor supplied patch.
http://www.vandyke.com/download/securecrt/index.html

About Security-Assessment.com

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and its team have previously identified a number of vulnerabilities in public and private software vendors products.

For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093