## NeoErudition Technologies

## By: Lawrence LaVigne administrator@neoerudition.net

Vulnerability: CGI-Telnet 1.0 By: Rhohitab Batra Http://www.rohitab.com

Remote: YES Risk: HIGH

CGI-Telnet is a CGI script that allows you to execute commands on your web server. As it sounds it is a telnet script that runs and is vulnerable on both UNIX and NT.

Cgitelnet.pl is kept in /cgi-bin/, accessible by web browser via the path <a href="http://www.domain.com/cgi-bin/cgitelnet.pl">http://www.domain.com/cgi-bin/cgitelnet.pl</a> along with its password file default.pass, accessible by web browser via the path <a href="http://www.domain.com/cgi-bin/dir/default.pass">http://www.domain.com/cgi-bin/dir/default.pass</a>.

The default password for cgitelnet is "changeme" and is DES encrypted. Once changed the new password is kept in default.pass along with any other added user accounts. Default.pass appears as:

# UserID: Password: View: Add: Del: Mod: Admin

webmaster:fvGAdIbemtCkI:1:1:1:1:1 admin:.FRGHgutWnVQA:1:1:1:1:1

CGI-Telnet does not enforce secure passwords.