Amendment: In mid summer of 2003 I had released a hasty paper about cgitelnet.pl's issues that where not entirely accurate and contained results of an audit preformed on DBMan which resulted in an inaccurate release of a security paper about cgitelnet.pl. I apologize to both Rohitab Batra of cgitelnet.pl and its community for this.

NeoErudition Technologies

By: Lawrence LaVigne
administrator@neoerudition.net

Software: CGI-Telnet v1.0 By: Rohitab Batra http://www.rohitab.com
Remote: Yes
Risk : Medium to High

Overview: CGI-Telnet is a CGI script that allows you to execute commands on your web server. It is a useful tool if you don't have telnet access to your server.

Cgitelnet.pl allows for single character or even blank, unencrypted passwords and does not limit bad login attempts, allowing for unlimited login/password bruteforce attempts.

Cgitelnet.pl is accessible by browser via path http://www.domain.com/cgi-bin/cgitelnet.pl

Software: DBMan By: http://www.gossamer-threads.com
Remote: Yes
Risk : Medium to High

Overview: DBMan is a full-featured Database Manager that provides a web interface to add, remove, modify or view records in a flatfile ASCII database.

DBMan makes its DES Encrypted "flatfile ASCII" password available through a browser via the path http://www.domain.com/cgi-bin/dbman/default.pass or http://www.domain.com/~user/cgi-bin/dbman/default.pass which does not enforce nor suggest use of secure passwords.

Example default.pass:

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

In addition to default.pass you can also find the "flatfile ASCII" files:

```
db.cgi              (755)       -rwxr--r--
html.pl             (644)       -rw-r--r--
auth.pl             (644)       -rw-r--r--
default.cfg         (644)       -rw-r--r--
default.pass        (666)       -rw-rw-rw-
default.count       (666)       -rw-rw-rw-
default.log         (666)       -rw-rw-rw-
default.db          (666)       -rw-rw-rw
auth                (777)       -drwxrwxrwx
```

When both authors where informed about these concerns, Rohitab Batra of cgitelnet had delivered a rapid, professional reply and carried out a lengthy discussion about cgitelnet. Rohitab did make a valid point of it is in the end-users responsibility to attend to his/her secure use of cgi scripts. While I partially agree with this point of view and cgitelnet is

freeware, there is just no patch for human stupidity and I strongly feel that if remote service software is going to be made available to the public, one should apply at least standard security features and not add to the already existing abundance of insecure remote software plaguing the net.

DBMan's gossamer-threads are yet to reply.

On several occasions I have encountered servers sporting both cgitelnet.pl and DBMan's default.pass. On each of these occasions the user had applied the same cgitelnet passwords to dbman which resulted in DES Encrypted passwords available in default.pass that could be cracked and used to gain access to the server through cgitelnet.pl

A likely attack may carry out as follows:

- Attacker does a mass scan (google ?) for web servers running cgi-telnet and dbman.
- Attacker connects to www.victim.com/cgi-bin/cgitelnet.pl to confirm it is running cgitelnet
- Attacker connects to www.victim.com/cgi-bin/dbman/default.pass
- Attacker copies default.pass and loads into password cracker of choice and waits briefly for successful crack.
- Attacker connects to www.victim.com/cgi-bin/cgitelnet.pl and loads accurate credentials into login/password fields to gain user or administrative access.