



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Hacker Tools, Techniques, Exploits, and Incident Handling (Security 504)"  
at <http://www.giac.org/registration/gcih>

SANS GCIH Practical Assignment  
Option 2 - **Document an exploit, vulnerability or malicious program**

**Thong.pl – Cisco Device Attack Script**

**by  
Glenn Johnson**

© SANS Institute 2000 - 2002, Author retains full rights.

## Exploit Details

---

### Summary

**Name:** Thong.pl

**Variants:** No known variants

**Operating System:** Various Cisco IOS and Catalyst switches

**Protocols/Services:** Multiple services including SSH and HTTP

**Brief Description:** Thong is a very simple tool to automate various attacks on Cisco routers and switches.

---

## Introduction and Description

---

### Introduction

Thong.pl is a Perl script written by hypoclear and posted at <http://hypoclear.cjb.net> on January 24, 2001. Thong is a very simple Perl program that serves as a virtual 'Swiss Army knife' for automating various attacks against Cisco routers and switches.

Thong can automated four different attacks against Cisco router and switch products:

1. Cisco Catalyst SSH Protocol Mismatch vulnerability (Cisco bug ID CSCds85763)
2. Cisco 675 Web Administration Denial of Service Vulnerability (BugTraq ID: 2012)
3. Cisco Catalyst 3500 XL Remote Arbitrary Command Execution Vulnerability (BugTraq ID:1846)
4. Cisco IOS HTTP Server Quesry Vulnerability (Cisco bug ID CSCdr91706)

The problem with this script is that it is ridiculously simple. In its current form it is powerful enough to cause significant damage to a number of key components in most company's infrastructure. With a little work, an inexperienced Perl programmer would be able to extend the scripts capabilities and corresponding destructive power.

This is significant for a couple of reasons. Many security professionals refer to 'script kiddies' with little to no respect. Implicit in this attitude is an assumption that the 'real' hackers are the gifted few that concentrate on a small number of targets that suit their own ends.

---

---

Thong.pl is an example of an extensible piece of code that is simple, intuitive and destructive. This type of application blurs the lines between ‘script kiddie’ and ‘real’ hacker. A newcomer to Perl could spend a weekend with an O’Reilly book and come up with a number of nefarious variants that could target your infrastructure.

---

## Protocol Description

---

### Secure Shell (SSH)

Thong.pl exploits two protocols, SSH (specifically SSH1) and HTTP. A discussion of these protocols follows:

#### *Overview*

SSH1 is a program that facilitates “strong authentication and secure communications over an insecure network”<sup>1</sup>. This protocol can replace the telnet, rlogin, rsh, rcp commands on Unix and Unix variants (hereafter “Unix will serve as a euphemism for all xNix variants) clients with equivalent functionality over a secure (encrypted) channel.

This protocol also provides a means of tunneling X windows traffic over the same secure channel. The secure channel is provided by one of four types of encryption:

- DES
- 3DES
- IDEA
- Blowfish

The server supports all four types and allows the client to select which encryption type to use for the entire session. Once the session is established, the user (or machine, for host base authentication) authenticates with the server using one of the supported authentication methods.

---

<sup>1</sup> IETF Draft Document “The SSH (Secure Shell) Remote Login Protocol, T. Ylonen, November 15, 1995, page 1.

---

SSH1 provides many kinds of authentication options to the administrator:

- /etc/passwd (or /etc/shadow) on Unix.
- Public Key (RSA)
- Kerberos
- Host based (.rhosts or /etc/hosts.equiv)

The client and server communicate over a static TCP socket connection on port 22. The communication is bi-directional over this port. The client always initiates the connection, and multiple clients can connect to the same server/port combination.

### ***Session Initiation***

In order to understand the exploit that thong.pl takes advantage of, an understanding is required of the session initiation process of secure shell. The session is initiated using the following method:

1. The client opens a socket connection to TCP port 22 on the server.
2. The server accepts the connection and responds with a packet that details version information and an identification string in clear text.
3. The client reads the server's packet and responds with its own identification.

*Note: The reason why they exchange this information is to “validate that the connection was to the correct port, declare the protocol version number used and to declare the software version number used on each side (for debugging purposes)”<sup>2</sup>*

4. After the protocol and version negotiation, both sides switch to a packet based binary protocol and follow these steps to establish the secure channel:
  - a. The server sends its host key (predefined in the sever setup process), its server key (periodically generated) and other information to the client.

- 
- b. The client receives these two keys and reads the other information in the packet. It looks for the encryption types that are supported by the server and selects an encryption algorithm that it also supports.
  - c. The client generates its own session key then encrypts this key using the keys received from the server.
  - d. Both sides turn on encryption using the method selected by the client.
  - e. The server sends an encrypted confirmation back to the client.
5. Once the secure channel is established, the client begins the authentication process defined by the server.
- 

**Hyper Text  
Transfer  
Protocol  
(HTTP)**

**Introduction**

The vulnerabilities that 'thong' leverages on Cisco hardware using HTTP are application or implementation specific vulnerabilities. This is somewhat true for the SSH vulnerabilities, although I think that the ssh protocol shares some responsibility in the particular vulnerability discussed below.

The HTTP protocol is not at fault for these vulnerabilities any more than the TCP protocol is at fault. This issue is the lack of error checking implemented in the HTTP service within Cisco equipment. The HTTP server is a relatively recent addition to the Cisco IOS and as such is experiencing the growing pains associated with a new software rollout.

It may be helpful to take a few minutes and recap the HTTP protocol to give us some more background as to the nature of the attack any why it is so effective.

---

<sup>2</sup> Ibid

## Overview

HTTP is an application level protocol that facilitates information annotation, search, update and exchange over a network. The protocol is written to be independent of specific reliable lower layer protocols that move it between client and server systems. The genius of the protocol is its simplicity and flexibility.

HTTP defines an open command set that depends upon structured references in the form of Uniform Resource Identifiers (URIs) to describe the location (URL) and names (URNs) of the targets of the commands. These terms are defined below:

- URLs (Uniform Resource Locators) – “the compact representation of the location and access method for a resource available via the Internet. When embedded within a base document, a URL in its absolute form may contain a great deal of information which is already known from the context of that base document's retrieval, including the scheme, network location, and parts of the url-path.”<sup>3</sup>
- URNs (Uniform Resource Names) – “provide a globally unique, persistent identifier used for recognition, for access to characteristics of the resource or for access to the resource itself”<sup>4</sup>

HTTP messages are sent in a format similar to Internet mail and relies heavily on the definitions for MIME (Multipurpose Internet Mail Extensions). The protocol is used as a generic transport or gateway protocol between user agents and FTP, SMTP, NNTP, Gopher and WAIS.<sup>5</sup>

---

<sup>3</sup> RFC 1808, Relative Uniform Resource Locators, R. Fielding pg. 1

<sup>4</sup> RFC 1737, Functional Requirements for Uniform Resource Names, K. Sollins +L. Masinter pg 3.

<sup>5</sup> RFC 1945, Hypertext Transfer Protocol -- HTTP 1.0, T. Berners-Lee et.al. pg. 3

---

## HTTP Protocol

The HTTP protocol is architected around the request/response paradigm. It is a client/server model in which communication is always initiated from the client. The connection is established in the following way<sup>6</sup>:

*The client:*

1. Establishes a connection with the server, traditionally over TCP port 80, although neither the port nor the TCP/IP protocol is specified by the standard.
2. The client sends a request to the server in the form of a command, or method, a location specification (URI).
3. The location specification is followed by a “MIME-like” message containing additional information that will help the server identify the intent of the client’s request.

The server:

1. Responds to the client with status information that includes the protocol version of the message, a success or error code.
2. The server sends a “Mime-like” message containing the servers information metadata and data.

Keep in mind that this describes the HTTP message exchange, not the information flow over any particular protocol. HTTP is usually implemented on top of TCP, and the preceding description of the message flow could take a great number of packets in each direction to realize a complete HTTP message exchange.

---

<sup>6</sup> Ibid, pg



## Description of the Variants

---

There are no known variants to this exploit at this time. However this script is pregnant with possibility. The script has a number of limitations that could easily be eliminated with an afternoon or two of programming. These suggestions are listed below:

- In its current form, the script can only target one IP address at a time. It would be relatively easy to change the command line option from a single host ip address to an address range that supports wild cards and/or read a text file containing target IPs.
  - The script can only be run in interactive mode, include a switch to run this in non-interactive mode and cycle through the list of IPs gleaned from the previous enhancement.
  - The script is limited to the specific vulnerabilities listed in this paper, it would be trivial to add an option to pass a user-specified string to a user specified port
- 

## How the Exploit Works

© SANS Institute 2000 - 2002, Author retains full rights.

## Denial of Service

The thong.pl script is a prime example of the ‘double-edged’ nature of security information. The exploit was written in response to Cisco’s announcements of DOS vulnerabilities in their switch and router operating systems. Hypoclear attributes the genesis of the exploit script to articles on the “www.securityfocus.com” web site.

The exploit leverages three specific DOS vulnerabilities in the different Cisco products. These are detailed below:

1. **SSH Protocol Mismatch** - This vulnerability affects Cisco Catalyst switches in the 4000, 5000 and 6000 series. All switches running version 6.1 or earlier of the OS are affected.

Cisco Catalyst switches and routers are all capable of running SSH as an option to secure the administration channel. All of the Cisco products have the capability of being managed from the command line, typically from a telnet session. Telnet access is inherently insecure for a number of reasons including a lack of strong authentication mechanisms and the fact that all information passes over the wire in clear-text format.

Cisco has made provision to make interactive configuration more secure by augmenting the default authentication method with more secure options (e.g. TACACS+ and RADIUS) as well as providing for encrypted interactive sessions via SSH.

Our discussion on the session initiation for the SSH protocol highlighted the expected behavior for a SSH client. Specifically, the client opens up a socket on port 22 TCP, the server immediately responds with an identification packet and the client responds back with version information of its own.

This particular bug in the Catalyst operating system results from the fact that the server does not know how to handle a packet from the client that does not contain version information. Thong.pl initiates the appropriate socket connection with the SSH server and responds back with a packet over TCP/Port 22, with a text string containing “This ain’t SSH”.

The server doesn’t know what to do with this response and the “switch might cause a "protocol mismatch" error, resulting in a supervisor engine failure. The supervisor engine failure causes the switch to fail to pass traffic and reboots the switch”<sup>7</sup>

---

<sup>7</sup> <http://www.cisco.com/warp/public/707/catalyst-ssh-protocolmismatch-pub.shtml>

- 
2. **Cisco 675 Web Admin** - A vulnerability exists in the 675 DSL router that permits a total denial of service against the router when presented with a malformed HTTP GET request.

Cisco added the capability to administer its switches and routers from a web browser interface. With every new capability comes the potential for additional exploits. This particular capability is a case in point.

According to Cisco, "Once connected via telnet to the Web Administration Interface, issuing the command "GET ? \n \n" will crash the telnet session as well as the router, requiring it be power cycled before resuming normal operation."<sup>8</sup>

In textbook fashion, thong opens a TCP socket connection to port 80 of the victims IP address and passes this particular string to the router.

3. **Cisco IOS HTTP Server Query** – Cisco routers and switches running IOS 12.0 through 12.1 (inclusive) are susceptible to a denial of service exploit when a particular HTTP GET request is submitted to the device and the enable password is supplied.

Thong.pl creates a TCP connection to the victim's IP address on port 80, sends "GET /error?/ HTTP/1.0\n\n" to the device. The attacker supplied the enable password and the switch or router will halt and reload. In view of the surprising number of switches and routers that have very simple enable passwords (or none at all) this attack continues to be a threat to environments that do protect themselves properly.

Cisco explains that the reason for the problem: "the meaning of a question mark when it appears adjacent to a "/" (slash) character cannot be determined properly by the URI parser in affected versions of Cisco IOS software. When a URI containing "?/" is presented to the HTTP service on the router and a valid enable password is supplied, the router enters an infinite loop. A watchdog timer expires two minutes later and forces the router to crash and reload. The router continue to be vulnerable to this defect as long as it is running an affected IOS software release and the enable password is known."<sup>9</sup>

---

<sup>8</sup> <http://www.securityfocus.com/bid/2012>

<sup>9</sup> <http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>

**Enable Access** The third menu option for this attack script allows an anonymous attacker to execute privileged level commands on a 3500XL switch. Any of these switches that run the web administration interface are vulnerable this attack.

Thong opens a TCP socket connection to port 80 and allows the user to execute arbitrary commands against the switch in question or will provide a default command. The default command is a “show config” (“GET /exec/show/config/cr HTTP/1.0\n\n”) that will display the running configuration, including SNMP information, passwords and VLAN configuration.

Any valid switch IOS command can be executed from within the thong.pl script. Potentially damaging commands for DOS attacks, network discovery commands like ping or traceroute as well as telnet, ftp and tftp commands to inside hosts.

---

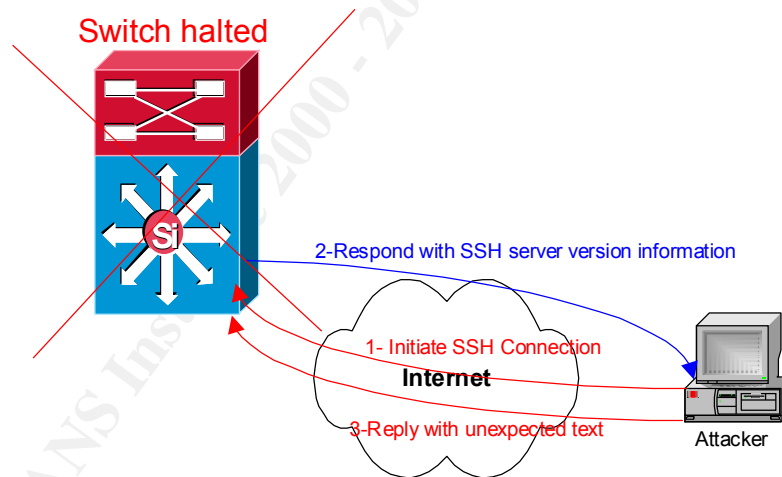
## Diagrams

---

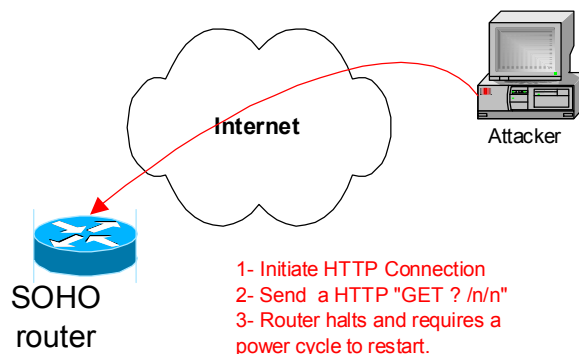
The following illustrate the attack options in this script:

---

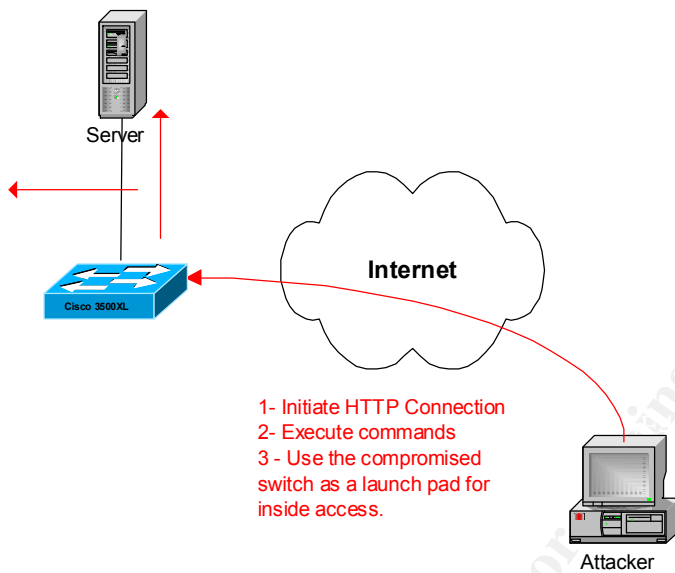
### Option 1) SSH DOS Vulnerability



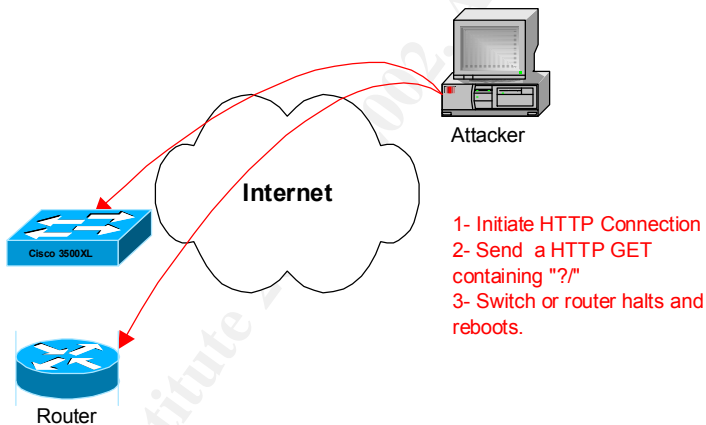
### Option 2) HTTP GET DOS against 675 DSL Router



**Option 3)  
EXEC  
Compromise on  
3500XL  
Switches**



**Option 4) DOS  
Against IOS  
12.0-12.1**



## How to Use This (These) Exploit(s)

---

### SSH DOS against Catalyst Switches

1. Execute `/usr/local/bin/perl ~/exploits/thong.pl -h <target host running SSH>`
  2. You are presented with the following menu options:
    1. 12-13-00 - Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability
    2. 11-28-00 - Cisco 675 Web Administration Denial of Service Vulnerability
    3. 10-26-00 - Cisco Catalyst 3500 XL Remote Arbitrary Command
    4. 10-25-00 - Cisco IOS Software HTTP Request DoS Vulnerability
  3. Select #1
- 

### HTTP GET DOS Against Cisco 675 Routers

1. Execute `/usr/local/bin/perl ~/exploits/thong.pl -h <target 675 router running http>`
  2. You are presented with the following menu options:
    1. 12-13-00 - Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability
    2. 11-28-00 - Cisco 675 Web Administration Denial of Service Vulnerability
    3. 10-26-00 - Cisco Catalyst 3500 XL Remote Arbitrary Command
    4. 10-25-00 - Cisco IOS Software HTTP Request DoS Vulnerability
  3. Select #2
- 

### Arbitrary Commands against a Catalyst 3500XL

1. Execute `/usr/local/bin/perl ~/exploits/thong.pl -h <Cisco Catalyst 3500 >`
  2. You are presented with the following menu options:
    1. 12-13-00 - Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability
    2. 11-28-00 - Cisco 675 Web Administration Denial of Service Vulnerability
    3. 10-26-00 - Cisco Catalyst 3500 XL Remote Arbitrary Command
    4. 10-25-00 - Cisco IOS Software HTTP Request DoS Vulnerability
  3. Select #3
  4. Select 'D' for Default or type in a custom command to execute on the Cisco switch. Results will be displayed on STDOUT.
- 

### Cisco IOS HTTP DOS attack

1. Execute `/usr/local/bin/perl ~/exploits/thong.pl -h <target host running Cisco IOS 12.0 - 12.1>`
2. You are presented with the following menu options:
  1. 12-13-00 - Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability
  2. 11-28-00 - Cisco 675 Web Administration Denial of Service Vulnerability
  3. 10-26-00 - Cisco Catalyst 3500 XL Remote Arbitrary Command
  4. 10-25-00 - Cisco IOS Software HTTP Request DoS Vulnerability
3. Select #4
4. Supply enable password.

## Signatures of the Attacks

---

**SSH DOS  
Attack**

This attack is particularly pernicious in that any text sent to the server as a result of the session initiation, other than the version information will result in the denial of service being successful. Since different clients can respond with different version information, it is practically impossible to catch this attack while in progress.

Should you wish to write a SNORT filter to analyze post mortem information, capture all SSH session initiation conversations through the first 10 packets or so.

---

**HTTP DOS  
against 675  
Routers**

This attack will succeed on a single “GET ?\n\n” string passed to the 675 router. These routers typically reside in small office/home office environments where it is not practical to implement an IDS. It is much more effective to implement the workaround for this issue.

---

**Cisco Catalyst  
3500XL  
Arbitrary  
Command**

This attack has no signature. Legitimate traffic and illegitimate traffic will look the same over the wire. The only way to detect it is to identify which hosts should have HTTP access to these switches and alert on all other HTTP access. It would be much more effective to implement the workaround on this issue.

---

**HTTP DOS  
Vulnerability  
for Cisco IOS  
12.0 – 12.1**

The signature for this attack is the “?” combination in the HTTP streams destined for the router. This signature may produce false positives since there are instances where that combination will occur in the course of legitimate access.

---

## How to Protect Against These Attacks

---

**SSH DOS Attack**

Upgrade your Catalyst OS to a version of code greater than or equal to 6.1(1.c). Alternatively, you can disable the SSH server on your switch, this workaround is not recommended since it introduces other security problems into your network.

---

**HTTP DOS against 675 Routers**

The only way to protect against this attack is to disable the HTTP Admin capability. Use the following command sequence from enable mode:

```
cbos# set web disabled
cbos# write
cbos# reboot
```

---

**Cisco Catalyst 3500XL Arbitrary Command**

As of this writing, there is no known software fix for this problem. The only workaround is to disable the web admin interface on the switch:

```
Switch#>conf t
Switch (config) no ip http-server
Switch (config) end
```

---

**HTTP DOS Vulnerability for Cisco IOS 12.0 – 12.1**

Once again, there are two workarounds for this vulnerability, upgrading the IOS and disabling the HTTP admin interface. Versions of the IOS greater than 12.1 are not vulnerable to this attack.

---

## Source code/Pseudo Code

---

**Source Code**

The source code can be found on hypoclear's web site:  
<http://hypoclear.cjb.net/>

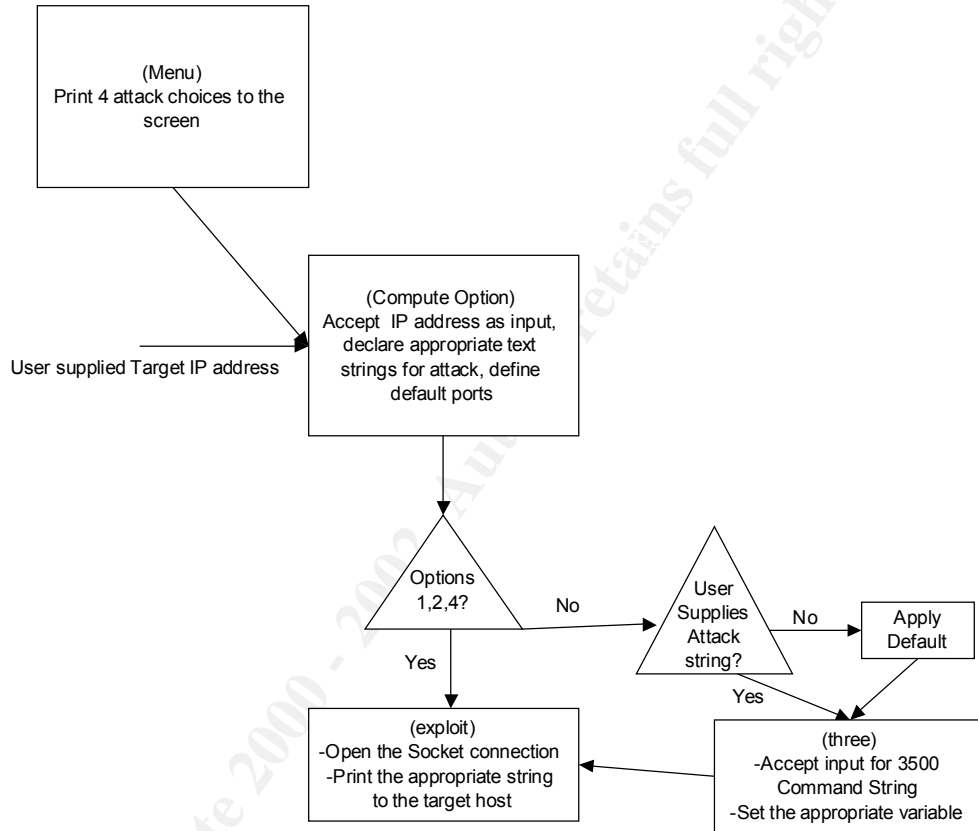
---



**Pseudo Code**

The attack script only takes one argument, the target host IP address, delimited by a “-h”

The flow for the script follows:



**Additional Information**

---

Additional information on the exploits can be found in Appendix A.

---

## Appendix A– Vulnerability Details

---

© SANS Institute 2000 - 2002, Author retains full rights.

## **Menu Option 1)** Cisco Catalyst SSH Protocol Mismatch Vulnerability

### **Summary**

Non-Secure Shell (SSH) connection attempts to an enabled SSH service on a Cisco Catalyst 6000, 5000, or 4000 switch might cause a "protocol mismatch" error, resulting in a supervisor engine failure. The supervisor engine failure causes the switch to fail to pass traffic and reboots the switch. This problem is resolved in release 6.1(1c). Due to a very limited number of customer downloads, Cisco has chosen to notify affected customers directly.

This vulnerability has been assigned Cisco bug ID CSCds85763.

The full text of this advisory can be viewed at:  
<http://www.cisco.com/warp/public/707/catalyst-ssh-protocolmismatch-pub.shtml>

### **Details**

Non SSH protocol connection attempts to the SSH service cause a "protocol mismatch" error, which causes a switch to reload. SSH is not enabled by default, and must be configured by the administrator.

To verify if your image is affected, run the command "show version". If the image filename is listed above, and you have enabled SSH, you are affected by this vulnerability and should upgrade to a fixed version immediately.

### **Impact**

This vulnerability enables a Denial of Service attack on the Catalyst switch.

### **Software Versions and Fixes**

This defect is resolved in Cisco Catalyst version 6.1(1c). Previous affected versions will be deferred, and will no longer be available for customer download.

### **Workarounds**

The workaround for this vulnerability is to disable SSH service. For most customers using this image, SSH support is necessary, so the recommended action is to upgrade to a fixed version.

---

**Menu  
Option 2)**

Cisco 675 Web Administration Denial of Service Vulnerability

BugTraq ID: 2012

Remote: Yes

Date Published: 2000-11-28

Relevant URL:

<http://www.securityfocus.com/bid/2012>

Summary:

The Cisco 675 DSL Router is a popular DSL router in wide use and distributed to major telco's for their SOHO clients.

A vulnerability exists in the Cisco 675 DSL Router that could allow a remote attacker to initiate a Denial of Service attack against the router requiring it to be power cycled in order to resume normal operation.

If the Cisco 675 DSL Router has the Web Administration Interface enabled,

a remote attacker could telnet to the router and issue a simple malformed

HTTP GET request. Once connected via telnet to the Web Administration

Interface, issuing the command GET ? \n \n will crash the telnet session

as well as the router, requiring it be power cycled before resuming normal operation.

It is possible, though not tested, that other Cisco routers in this series (673, 675e, 676, and 678) are also vulnerable.

Currently, the only available solution is to disable the Web Based Administration Interface via the Router by issuing the following commands:

```
cbos# set web disabled
cbos# write
cbos# reboot
```

---

**Menu  
Option 3**

Cisco Catalyst 3500 XL Remote Arbitrary Command Execution  
Vulnerability

BugTraq ID: 1846

Remote: Yes

Date Published: 2000-10-26

Relevant URL:

<http://www.securityfocus.com/bid/1846>

Summary:

Cisco Catalyst 3500 XL is a high speed switch implemented in local area networks.

A vulnerability exists in the webserver configuration interface which will allow an anonymous user to execute commands. A http request which includes /exec and a known filename will reveal the contents of the particular file. In addition to disclosing the contents of files, this vulnerability could allow a user to execute arbitrary code.

Successful exploitation of this vulnerability could lead to a complete compromise of the host.

Example:

`http://target/exec/show/config/cr`

This URL will disclose the user password configuration file.

---

## Menu Option 4)

### Cisco IOS HTTP Server Query Vulnerability

#### Summary

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to "http://router-ip/anytext?/" is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.

The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.

This vulnerability can only be exploited if the enable password is known or not set.

The complete advisory is available at <http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml> .

#### Affected Products

The following products are affected if they run a Cisco IOS software release that has the defect. To determine if a Cisco product is running an affected IOS, log in to the device and issue the command

show version. Cisco IOS software will identify itself as "Internetwork Operating System Software" or "IOS (tm)" software and will display a

version number. Other Cisco devices either will not have the command

show version, or will give different output. Compare the version number obtained from the router with the versions presented in the Software Versions and Fixes section below.

---

Cisco devices that may be running with affected IOS software releases

include:

- \* Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, ubr900, 1000, 1400, 1500, 1600, 1700, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200, ubr7200, 7500, and 12000 series.
- \* Most recent versions of the LS1010 ATM switch.
- \* The Catalyst 6000 if it is running IOS.
- \* The Catalyst 2900XL LAN switch only if it is running IOS.
- \* The Cisco DistributedDirector.

For some products, the affected software releases are relatively new and may not be available on every device listed above.

If you are not running Cisco IOS software, you are not affected by this vulnerability.

Cisco products that do not run Cisco IOS software and are not affected

by this defect include, but are not limited to:

- \* 700 series dialup routers (750, 760, and 770 series) are not affected.
  - \* Catalyst 1900, 2800, 2900, 3000, and 5000 series LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected (see the Affected Products section above).
  - \* The Catalyst 6000 is not affected if it is not running IOS.
  - \* WAN switching products in the IGX and BPX lines are not affected.
  - \* The MGX (formerly known as the AXIS shelf) is not affected.
  - \* No host-based software is affected.
  - \* The Cisco PIX Firewall is not affected.
  - \* The Cisco LocalDirector is not affected.
  - \* The Cisco Cache Engine is not affected.
-

---

## Details

The HTTP server was introduced in IOS release 11.0 to extend router management to the worldwide Web. The "?" (question mark) character is defined in the HTML specifications as a delimiter for CGI arguments. It is also interpreted by the IOS command-line interface as a request for help.

As of Cisco IOS Software Release 12.0T, c

This vulnerability may only be exploited if the enable password is not set, it is well known, or it can be guessed.

In rare cases, an affected device fails to reload, which means an administrator must physically cycle the power to resume operation.

The HTTP server is not enabled by default except on unconfigured Cisco model 1003, 1004, and 1005 routers. Once initial access is granted to configure the router, the customer may set an enable password, and disable or limit access to the HTTP server by changing the configuration. Once the new configuration has been saved, the HTTP server will not be enabled when the router restarts.

© SANS Institute 2000



---

## Impact

An affected Cisco IOS device that is operating with the HTTP service enabled and is not protected by having the enable password configured can be forced to halt for up to two minutes and then reload. The vulnerability can be exercised repeatedly, possibly creating a denial of service (DOS) attack, unless the service is disabled, the enable

password is set, or the router is upgraded to a fixed release.

In instances in which a router at a remote location fails to reload, an administrator must visit the site to enable the device to recover from the defect.

## Software Versions and Fixes

The following table summarizes the Cisco IOS software releases affected by the defect described in this notice and scheduled dates on which the earliest corresponding fixed releases will be available. Dates are tentative and subject to change.

Each table row shows the earliest release that contains the fix in the "Rebuild", "Interim", or "Maintenance" columns, presented in release number order.

A Maintenance Release is the most heavily tested and highly recommended release.

A Rebuild Release is constructed from a previous maintenance or mainline release and contains a code fix for a specific defect.

Although it receives less testing than a maintenance release, it is built from a previous maintenance release and includes minimum changes to address a specific defect.

An Interim Release has much less testing than a maintenance release and should be selected only if no other suitable release fixes the defect.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release.

<http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>

## Workarounds

© SANS Institute 2000 - 2002, Author retains full rights.

# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



Community SANS Columbus SEC504	Columbus, OH	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS New York SEC504^	New York, NY	Nov 06, 2017 - Nov 11, 2017	Community SANS
Mentor Session AW - SEC504	Houston, TX	Nov 06, 2017 - Jan 29, 2018	Mentor
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Raleigh SEC504	Raleigh, NC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Amsterdam 2017	Amsterdam, Netherlands	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, Italy	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Toronto SEC504	Toronto, ON	Nov 13, 2017 - Nov 18, 2017	Community SANS
Mentor Session SEC504	Houston, TX	Nov 13, 2017 - Dec 11, 2017	Mentor
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MD	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Detroit SEC504~	Detroit, MI	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, Germany	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Honolulu SEC504	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC504	San Antonio, TX	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Community SANS Ottawa SEC504	Ottawa, ON	Jan 15, 2018 - Jan 20, 2018	Community SANS
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Community SANS St Louis SEC504	St Louis, MO	Jan 15, 2018 - Jan 20, 2018	Community SANS
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504 - 201801,	Jan 16, 2018 - Feb 22, 2018	vLive
SANS Dubai 2018	Dubai, United Arab Emirates	Jan 27, 2018 - Feb 01, 2018	Live Event