Licence Professionnelle SEICOM

Travaux dirigés

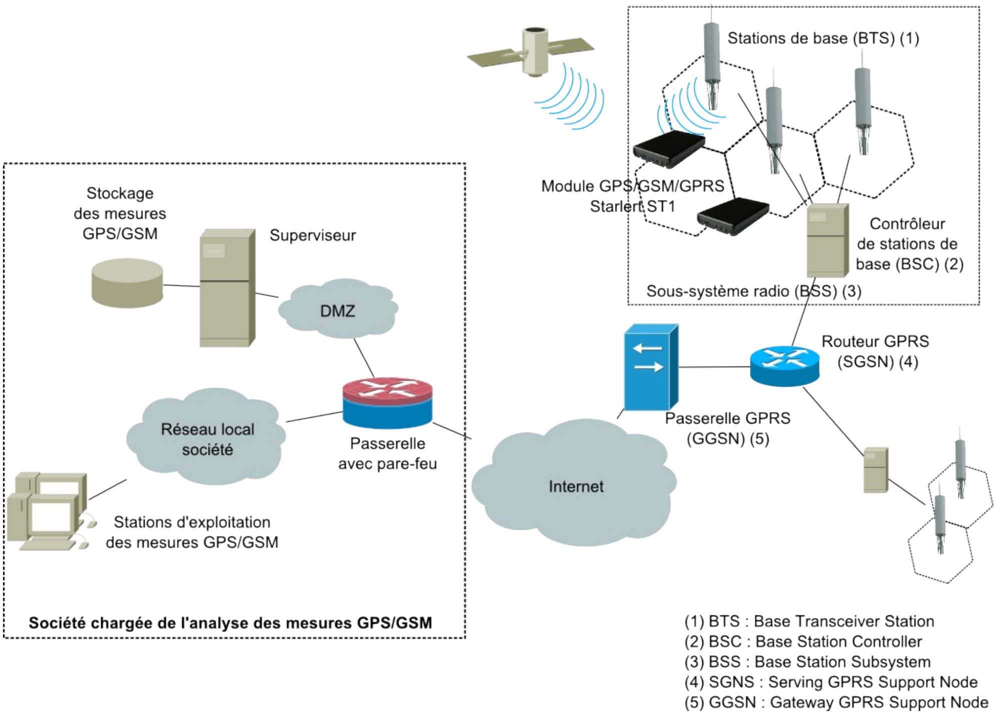
M3-6 : Réseaux et sécurité

Table des matières

1 - Présentation

On se propose d'étudier les différentes facettes de la sécurisation du système de Mesure de qualité d'un réseau mobile, thème de projet 2007 proposé par la société Panexdium.

Synoptique :


Stations de base (BTS) (1)
Module GPS/GSM/GPRS
Starlert ST1
Contrôleur
de stations de
base (BSC) (2)
Sous-système radio (BSS) (3)
Stockage
des mesures
GPS/GSM
Superviseur
DMZ
Réseau local
société
Passerelle
avec pare-feu
Stations d'exploitation
des mesures GPS/GSM
Société chargée de l'analyse des mesures GPS/GSM
Internet
Routeur GPRS
(SGSN) (4)
Passerelle GPRS
(GGSN) (5)
(1) BTS : Base Transceiver Station
(2) BSC : Base Station Controller
(3) BSS : Base Station Subsystem
(4) SGNS : Serving GPRS Support Node
(5) GGSN : Gateway GPRS Support Node

Question 1 : Identifiez, sur le synoptique, les différents éléments physiques de la chaîne de communication à prendre en compte dans l'audit de sécurité.

-
-
-
-
-

Question 2 : Pour chaque élément identifié, listez les menaces possibles et proposez une première solution.

Éléments	Menaces possibles	Solutions proposées

2 - Collecte d'informations

On donne le résultat de la collecte d'informations sur le serveur de la société Panexdium :

```
# nmap -v www.panexdium.com

Starting Nmap 4.20 ( http://insecure.org ) at 2007-03-08 23:35 CET
Initiating Parallel DNS resolution of 1 host. at 23:35
Completed Parallel DNS resolution of 1 host. at 23:35, 0.08s elapsed
Initiating SYN Stealth Scan at 23:35
Scanning 217.167.xx.xx [1697 ports]
Discovered open port 21/tcp on 217.167.xx.xx
Discovered open port 22/tcp on 217.167.xx.xx
Discovered open port 80/tcp on 217.167.xx.xx
Discovered open port 3306/tcp on 217.167.xx.xx
Completed SYN Stealth Scan at 23:36, 60.72s elapsed (1697 total ports)
Host 217.167.xx.xx appears to be up ... good.
Interesting ports on 217.167.xx.xx:
Not shown: 1687 filtered ports
PORT     STATE  SERVICE
20/tcp   closed   ❶
21/tcp   open     ❷
22/tcp   open     ❸
80/tcp   open     ❹
113/tcp  closed auth
3000/tcp closed ppp
3001/tcp closed nessusd
3005/tcp closed deslogin
3006/tcp closed deslogind
3306/tcp open   mysql

Nmap finished: 1 IP address (1 host up) scanned in 61.473 seconds
               Raw packets sent: 3394 (149.316KB) | Rcvd: 22 (1022B)
```

On donne un extrait du fichier de services `/etc/services` donnant le numéro de port associé au nom service :

```
chargen          19/tcp    # Character Generator
chargen          19/udp    # Character Generator
ftp-data         20/tcp    # File Transfer [Default Data]
ftp-data         20/udp    # File Transfer [Default Data]
ftp              21/tcp    # File Transfer [Control]
fsp              21/udp    # File Transfer [Control]
ssh              22/tcp    # SSH Remote Login Protocol
ssh              22/udp    # SSH Remote Login Protocol
telnet           23/tcp    # Telnet
telnet           23/udp    # Telnet
smtp             25/tcp    mail         # Simple Mail Transfer
smtp             25/udp    mail         # Simple Mail Transfer
vettcp           78/tcp    # vettcp
vettcp           78/udp    # vettcp
finger           79/tcp    # Finger
finger           79/udp    # Finger
http             80/tcp    # World Wide Web HTTP
http             80/udp    # World Wide Web HTTP
www              80/tcp    # World Wide Web HTTP
www              80/udp    # World Wide Web HTTP
www-http         80/tcp    # World Wide Web HTTP
www-http         80/udp    # World Wide Web HTTP
hosts2-ns        81/tcp    # HOSTS2 Name Server
```

```
hosts2-ns         81/udp    # HOSTS2 Name Server
xfer              82/tcp    # XFER Utility
xfer              82/udp    # XFER Utility
```

Question 3 : Donnez la commande permettant de collecter l'information sur le serveur :

-

Question 4 : Donnez le nombre de ports :

- Au total :
- Ouverts :
- Fermés :
- Filtrés :

Question 5 : Donnez, pour les services suivants identifiés lors de la collecte, son nom et son utilité :

❶

❷

❸

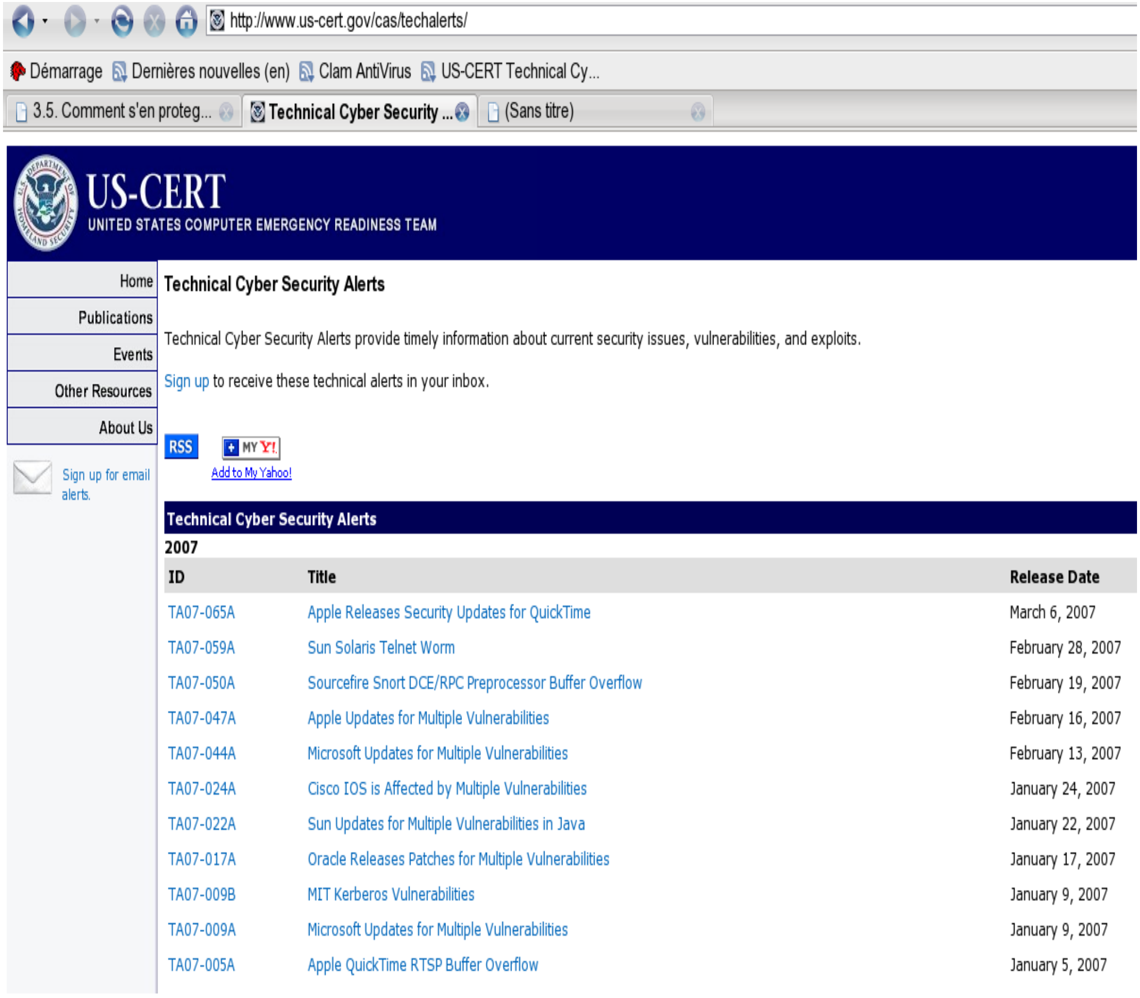
❹

Question 6 : Combien de données ont été envoyées par le scanner de port au serveur pour effectuer son test ?

-

3 - Les failles applicatives : veille sécurité

L'administrateur système et réseaux de la société a repéré une information susceptible de concerner la sécurité de son système d'information lors d'une veille sécurité sur le site du CERT :


http://www.us-cert.gov/cas/techalerts/
Démarrage
Dernières nouvelles (en)
Clam AntiVirus
US-CERT Technical Cy...
3.5. Comment s'en proteg...
Technical Cyber Security ...
(Sans titre)
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
Home
Publications
Events
Other Resources
About Us
Sign up for email alerts.
RSS
MY Y!
Add to My Yahoo!

Technical Cyber Security Alerts

Technical Cyber Security Alerts provide timely information about current security issues, vulnerabilities, and exploits.

Sign up to receive these technical alerts in your inbox.

Technical Cyber Security Alerts

2007

ID	Title	Release Date
TA07-065A	Apple Releases Security Updates for QuickTime	March 6, 2007
TA07-059A	Sun Solaris Telnet Worm	February 28, 2007
TA07-050A	Sourcefire Snort DCE/RPC Preprocessor Buffer Overflow	February 19, 2007
TA07-047A	Apple Updates for Multiple Vulnerabilities	February 16, 2007
TA07-044A	Microsoft Updates for Multiple Vulnerabilities	February 13, 2007
TA07-024A	Cisco IOS is Affected by Multiple Vulnerabilities	January 24, 2007
TA07-022A	Sun Updates for Multiple Vulnerabilities in Java	January 22, 2007
TA07-017A	Oracle Releases Patches for Multiple Vulnerabilities	January 17, 2007
TA07-009B	MIT Kerberos Vulnerabilities	January 9, 2007
TA07-009A	Microsoft Updates for Multiple Vulnerabilities	January 9, 2007
TA07-005A	Apple QuickTime RTSP Buffer Overflow	January 5, 2007

Question 7 : Repérez l'alerte de sécurité pouvant concerner l'infrastructure réseau de la société :

-

L'administrateur veut en avoir le cœur net et décide de vérifier ses équipements :

Question 8 : En vous aidant de l'annexe 1, donnez les différentes étapes que l'administrateur suivra pour vérifier ses équipements :

-
-
-
-
-
-

Question 9 : En vous aidant de l'annexe 1, décrivez succinctement le risque encouru :

-

Question 10 : Donnez la commande à entrer sur l'équipement pour vérifier sa vulnérabilité :

-

Le résultat de la commande entrée sur l'équipement est la suivante :

```
Cisco IOS Software, C831 Software (C831-K9O3Y6-M), Version 12.3(2)XF, RELEASE
SOFTWARE (fc1)
Synched to technology version 12.3(3.5)T
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Mon 09-May-05 09:42 by ealyon

ROM: System Bootstrap, Version 12.2(11r)YV3, RELEASE SOFTWARE (fc2)
ROM:

Router uptime is 3 days, 18 hours, 41 minutes
System returned to ROM by power-on
System image file is "flash:c831-k9o3y6-mz.123-2.XF.bin"
```

Question 11 : En vous aidant de l'annexe 1, précisez si l'équipement est vulnérable et ce qu'il faut faire pour le protéger :

-

4 - Les failles applicatives : surveiller les services

La commande netstat donne le résultat suivant sur le superviseur de la DMZ audité :

```
# netstat -taupen | sort
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale  Adresse distante  Etat  Utilisatr  Inode      PID/Program name
tcp        0      0 0.0.0.0:111         0.0.0.0:*     LISTEN      0    11634      5075/portmap
tcp        0      0 0.0.0.0:139         0.0.0.0:*     LISTEN      0    13147      5668/smbd
tcp        0      0 0.0.0.0:143         0.0.0.0:*     LISTEN      0    12705      5473/xinetd
tcp        0      0 0.0.0.0:199         0.0.0.0:*     LISTEN      0    533008     1305/snmpd
tcp        0      0 0.0.0.0:25          0.0.0.0:*     LISTEN      0    5697058    30169/sendmail: acc
tcp        0      0 0.0.0.0:3306        0.0.0.0:*     LISTEN      0    12718      5471/mysqld
tcp        0      0 0.0.0.0:389         0.0.0.0:*     LISTEN      0    12521      5474/slapd
tcp        0      0 0.0.0.0:631         0.0.0.0:*     LISTEN      0    15262      5583/cupsd
tcp        0      0 0.0.0.0:713         0.0.0.0:*     LISTEN      0    13028      5625/rpc.mountd
tcp        0      0 0.0.0.0:901         0.0.0.0:*     LISTEN      0    12707      5473/xinetd
tcp        0      0 127.0.0.1:10024     0.0.0.0:*     LISTEN      0    13548      5801/amavisd
tcp        0      0 127.0.0.1:3310      0.0.0.0:*     LISTEN      65   12700      5343/clamd
tcp        0      0 192.168.x.x:46236   192.168.y.y:  ESTABLISHED 0    12527      5474/slapd
tcp        0      0 0.0.0.0:547         0.0.0.0:*     LISTEN     0    12587      5766/dhcpd
tcp        0      0 192.168.x.x:46248  192.168.z.z:389ESTABLISHED 0   3646339    2916/httpd2-prefork
```

Question 12 : Donnez le nom des services ayant une connexion active :

-

Question 13 : Identifier les services qu'il faut désactiver sur le serveur sachant que seul les services web, ftp, courrier, antivirus, base de données et annuaire LDAP sont autorisés.

-
-
-
-
-

5 - Les failles applicatives : repérer les risques

Question 14 : Complétez le tableau suivant avec les risques générés par l'installation et l'exploitation des services suivants dans un réseau local connecté à Internet ainsi que le type de protection à envisager.

Application à risque	Risques externes (Internet)	Risques internes (LAN)	Type de protection à envisager
Serveur web			
Applications web (CGI, PHP, etc)			
Serveur FTP			
Serveur DHCP			
Serveur de courrier (SMTP)			
Serveur de base de données			
Serveur Telnet/SSH			
Peer to Peer			
Applications Windows téléchargées sur un site autre que celui du concepteur			
Applications GNU/Linux téléchargées sur un site autre que celui du concepteur			.

6 - Le pare-feu

Le pare-feu est un dispositif situé à la frontière d'un réseau local qui permet de le protéger de certaines attaques pouvant venir de l'extérieur (ou de l'intérieur).

Le pare-feu individuel permet, lui, de protéger une machine contre certaines attaques dirigées contre elle-même. La commande suivante donne les règles du pare-feu pour le superviseur :

```
# iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  251 38010 ACCEPT     all  --  lo     any     anywhere             anywhere
 337K  499M ACCEPT     all  --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED
   27  3022 input_ext  all  --  eth1   any     anywhere             anywhere
    0     0 input_ext  all  --  eth1   any     anywhere             anywhere
    0     0 input_ext  all  --  any    any     anywhere             anywhere
    0     0 LOG        all  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 LOG level warning tcp-options ip-options prefix `SFW2-IN-ILL-TARGET '
    0     0 DROP       all  --  any    any     anywhere             anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 LOG level warning tcp-options ip-options prefix `SFW2-FWD-ILL-ROUTING '

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  252 38050 ACCEPT     all  --  any    lo      anywhere             anywhere
 187K   12M ACCEPT     all  --  any    any     anywhere             anywhere            state NEW,RELATED,ESTABLISHED
    0     0 LOG        all  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 LOG level warning tcp-options ip-options prefix `SFW2-OUT-ERROR '

Chain forward_ext (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain input_ext (3 references)
 pkts bytes target     prot opt in     out     source               destination
    4  1312 DROP       all  --  any    any     anywhere             anywhere            PKTTYPE = broadcast
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp source-quench
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            icmp echo-request
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED icmp echo-reply
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED icmp destination-unreachable
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED icmp time-exceeded
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED icmp parameter-problem
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED icmp timestamp-reply
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED icmp address-mask-reply
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED icmp protocol-unreachable
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere            state RELATED,ESTABLISHED icmp redirect
    0     0 LOG        tcp  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 tcp dpt:http flags:FIN,SYN,RST,ACK/SYN LOG level warning tcp-options ip-options prefix `SFW2-INext-
ACC-TCP '
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere            tcp dpt:http
    0     0 ACCEPT     udp  --  any    any     anywhere             anywhere            udp dpt:syslog
    0     0 ACCEPT     udp  --  any    any     anywhere             anywhere            udp dpt:tftp
    0     0 reject_func  tcp  --  any    any     anywhere             anywhere            tcp dpt:ident state NEW
    0     0 LOG        all  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 PKTTYPE = multicast LOG level warning tcp-options ip-options prefix `SFW2-INext-DROP-DEFLT '
    0     0 DROP       all  --  any    any     anywhere             anywhere            PKTTYPE = multicast
    0     0 LOG        tcp  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 tcp flags:FIN,SYN,RST,ACK/SYN LOG level warning tcp-options ip-options prefix `SFW2-INext-DROP-
DEFLT '
    0     0 LOG        icmp --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 LOG level warning tcp-options ip-options prefix `SFW2-INext-DROP-DEFLT '
   21  1630 LOG        udp  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 LOG level warning tcp-options ip-options prefix `SFW2-INext-DROP-DEFLT '
    2    80 LOG        all  --  any    any     anywhere             anywhere            limit: avg 3/min burst 5 state INVALID LOG level warning tcp-options ip-options prefix `SFW2-INext-DROP-DEFLT-INV '
   23  1710 DROP       all  --  any    any     anywhere             anywhere

Chain reject_func (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     tcp  --  any    any     anywhere             anywhere            reject-with tcp-reset
    0     0 REJECT     udp  --  any    any     anywhere             anywhere            reject-with icmp-port-unreachable
    0     0 REJECT     all  --  any    any     anywhere             anywhere            reject-with icmp-proto-unreachable
```

Question 15 : Quel sont les décisions possibles prise par le pare-feu pour un paquet donnée (cf. target) :

-
-
-
-

Question 16 : En s'intéressant uniquement à la chaîne INPUT, que se passe-t'il si un paquet http arrive sur l'interface eth1 ?

-

Question 17 : même question pour un paquet ftp ?

-

Question 18 : Donnez les ports ouvert sur le pare-feu :

-
-
-
-

ANNEXE 1 : Cisco Security Advisory: Crafted TCP Packet Can Cause Denial of Service

Document ID: 72318
Advisory ID: cisco-sa-20070124-crafted-tcp
http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml
1.2
Last Updated 2007 February 02 2100 UTC (GMT)
For Public Release 2007 January 24 1600 UTC (GMT)

Please provide your feedback on this document.

Contents

Summary

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.
This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.
Cisco has made free software available to address this vulnerability for affected customers.
This issue is documented as Cisco bug ID CSCek37177 (registered customers only) .
There are workarounds available to mitigate the effects of the vulnerability.
This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml.

Affected Products

Vulnerable Products

This issue affects all Cisco devices running Cisco IOS software. To be affected, devices must be configured to process Internet Protocol version 4 (IPv4) packets and receive TCP packets. Devices which run only Internet Protocol version 6 (IPv6) are not affected.
This vulnerability is present in all unfixed versions of Cisco IOS software, including versions 9.x, 10.x, 11.x and 12.x.

To determine the software running on a Cisco product, log in to the device and issue the "**show version**" command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS". On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the "**show version**" command or will give different output.

The following example identifies a Cisco product running Cisco IOS release 12.2(14)S16 with an installed image name of C7200-IS-M:

Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-IS-M), Version 12.2(14)S16, RELEASE SOFTWARE (fc1)

The release train label is "12.2".

The next example shows a product running IOS release 12.3(7)T12 with an image name of C7200-IK9S-M:

Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(7)T12, RELEASE SOFTWARE (fc1)

Additional information about Cisco IOS Banners is available at:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml#3

Products Confirmed Not Vulnerable

Cisco products that do not run IOS are unaffected by this vulnerability.

Cisco IOS-XR is not affected.

No other Cisco products are currently known to be affected by this vulnerability.

Details

TCP is the transport layer protocol designed to provide connection-oriented, reliable delivery of a data stream. To accomplish this, TCP uses a mixture of flags to indicate state and sequence numbers to identify the order in which the packets are to be reassembled. TCP also provides a number, called an acknowledgement number, that is used to indicate the sequence number of the next packet expected. The full specification of the TCP protocol can be found at http://www.ietf.org/rfc/rfc0793.txt.

Cisco IOS devices that are configured to receive TCP packets are exposed to this issue. This Advisory does not apply to traffic that is transiting the device.

Certain crafted packets destined to an IPv4 address assigned to a physical or virtual interface on a Cisco IOS device may cause the device to leak a small amount of memory. Over time, such a memory leak may lead to memory exhaustion and potentially degraded service.

Although this is an issue with TCP, it is not required to complete the TCP 3-way handshake in order for the memory leak to be triggered. Therefore, TCP packets with a spoofed source address may trigger the leak.

The following document contains additional information on how to identify if your router is suffering from a memory leak in Processor memory:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6f3a.shtml#tshoot2

Impact

Successful exploitation of the vulnerability may result in a small amount of processor memory to leak, which may lead to degraded service. This issue will not resolve over time, and will require a device reset to recover the leaked memory.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the device will not trigger this issue.

Software Version and Fixes

When considering software upgrades, also consult http://www.cisco.com/go/psirt and any subsequent advisories to determine exposure and a complete upgrade solution.

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. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL:
http://www.cisco.com/warp/public/620/1.html.

Note: There are three IOS security advisories and one field notice being published on January 24, 2007. Each advisory lists only the releases which fix the issue described in the advisory. A combined software table is available at http://www.cisco.com/warp/public/707/cisco-sa-20070124-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of January 24, 2007. Links for the advisories and field notice are listed here.

- http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml
- http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml
- http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml
- http://www.cisco.com/warp/public/770/fn62613.shtml

Requests for software rebuilds to include the change for Daylight Savings Time (DST) that will be implemented in March 2007 should be directed through the Technical Assistance Center (TAC), and this advisory should be used as reference.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Release	**Rebuild**	**Maintenance**
12.2YS	Vulnerable; migrate to 12.3(4)T13 or later	
12.2YT	Vulnerable; migrate to 12.3(19) or later	
12.2YU	Vulnerable; migrate to 12.3(4)T13 or later	
12.2YV	Vulnerable; migrate to 12.3(4)T13 or later	
12.2YW	Vulnerable; migrate to 12.3(4)T13 or later	
12.2YX	Vulnerable; migrate to 12.4(8) or later	
12.2YY	Vulnerable; migrate to 12.3(4)T13 or later	
12.2YZ	Vulnerable; migrate to 12.2(25)S12 or later; Available 12-Feb-07	
12.2ZA	Vulnerable; migrate to 12.2(18)SXD7a or later	
Affected 12.3-Based Release	**Rebuild**	**Maintenance**
12.3	12.3(10f)	12.3(19)
12.3B	Vulnerable; migrate to 12.3(11)T11 or later	
12.3BC	12.3(13a)BC6	
	12.3(17a)BC2	
12.3TPC	Vulnerable; contact TAC	
12.3XA	Vulnerable; contact TAC	
12.3XB	Vulnerable; migrate to 12.3(11)T11 or later	
12.3XC	Vulnerable; contact TAC	
12.3XD	Vulnerable; migrate to 12.3(11)T11 or later	
12.3XE	Vulnerable; contact TAC	
12.3XF	Vulnerable; migrate to 12.3(11)T11 or later	
12.3XG	Vulnerable; contact TAC	
12.3XH	Vulnerable; migrate to 12.3(11)T11 or later	
12.3XI	12.3(7)XI8	
12.3XJ	Vulnerable; migrate to 12.3(14)YX2 or later	

12.3XK	Vulnerable; migrate to 12.4(8) or later
12.3XQ	Vulnerable; migrate to 12.4(8) or later
12.3XR	Vulnerable; contact TAC
12.3XS	Vulnerable; migrate to 12.4(8) or later
12.3XU	Vulnerable; migrate to 12.4(2)T5 or later
12.3XW	Vulnerable; migrate to 12.3(14)YX2 or later
12.3XX	Vulnerable; migrate to 12.4(8) or later
12.3XY	Vulnerable; migrate to 12.4(8) or later
12.3YA	Vulnerable; contact TAC
12.3YD	Vulnerable; migrate to 12.4(2)T5 or later
12.4XE	All 12.4XE releases are fixed
12.4XG	All 12.4XG releases are fixed
12.4XJ	All 12.4XJ releases are fixed
12.4XP	All 12.4XP releases are fixed
12.4XT	All 12.4XT releases are fixed