



secure auditor

Audit Report

Vulnerability comparison by machine with solutions

Report Generated Time: 9/27/2011 At 2:59:18PM

Audit Name: : CiscoAudit(Sep 27 2011 2:55PM)

Description: : Cisco Audit Report

IP Count : 1

IPs: : 192.168.68.203



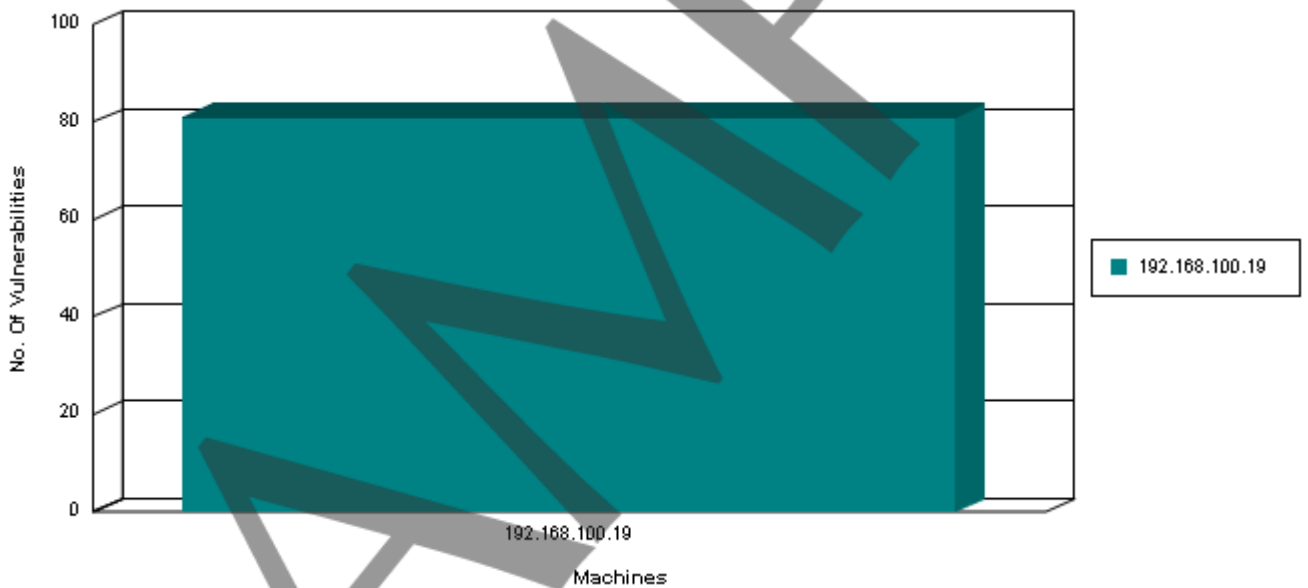


Vulnerability Comparison by machine with solutions

Report generated on 27-Sep-2011 at 2:59:18PM

Cisco Routers are normally placed at the center of the network, normally if the router is breached it takes the entire network down with it. A security scan was performed on your Cisco router or multiple Cisco routers. This audit report will give you a complete picture of your router security pasture. This review was performed on your network for single or multiple IP's with their number of audits regarding single or multiple routers. This Report shows audit detail for each router. This report is designed to provide a wide-ranging description of vulnerability found on specific audit performed. You can also review the summarized overview of the vulnerabilities discovered. This report covers the maximum researched and checked information about vulnerability including the aspect, ways and areas sensitive or unsafe and usually takes up by attackers. It is recommended to take a thorough review of vulnerabilities explored.

Machine(s) and Vulnerabilities



Summary Information

Machine IP	:	Number of Vulnerabilities
Total Vulnerabilities on : 192.168.68.203	=	81
Total Vulnerabilities :	=	81

Vulnerability Comparison by machine with solutions

Audit Performed: CiscoAudit(Sep 27 2011 2:55PM)**Selected Profile:** SCA**Machine :** 192.168.68.203**Risk Level :** High**Vulnerability Name** Access Class is not configured on VTY.**Vulnerability Description :**

On cisco routes use an access class for vty lines whenever possible. Because vty connections permit remote access to your router, they should be limited only to known network nodes.

Solution :

configuring VTY authentication with ACL If Policy does not required SSH.
SecureRoute1# config t
Enter configuration commands, one per line. End with CNTL/Z.
SecureRoute1 (config) # no access-list 90
SecureRoute1 (config) # access-list 90 deny any log
SecureRoute1 (config) # line vty 0 4
SecureRoute1 (config-line) # access-class 90 in
SecureRoute1 (config-line) # transport input ssh
SecureRoute1 (config-line) # login local
SecureRoute1 (config-line) # exec-timeout 0 1
SecureRoute1 (config-line) # no exec
SecureRoute1 (config-line) # end

Vulnerability Name Authentication Retry settings are not configuration for SSH**Vulnerability Description :**

This policy checks that the authentication retry limits for the SSH negotiation phase are set. The policy's defaults are based on the values configured.

Solution :

hostname (config)# (config)#ip ssh
authentication-retries <retries>
Step By Step
hostname # config t
Enter configuration commands, one per line. End with CNTL/Z.
hostname (config)#
hostname (config)# (config)#ip ssh
authentication-retries 2
hostname (config-line)# exit

Vulnerability Name Cisco Discovery Protocol (CDP) is enabled.**Vulnerability Description :**

CDP is a proprietary protocol that Cisco routers use to identify each other on a LAN segment. This is dangerous in that it allows any system on a directly connected segment to learn that the router is a Cisco device and to determine the model number and the Cisco IOS software version being run. This information may be used to design attacks against the router.

Solution :

In order to mitigate this vulnerability one should turn off CDP entirely, using the commands shown below in global configuration mode.
SecureRoute1 # config t
Enter configuration commands, one per line. End with CNTL/Z.
SecureRoute1 (config) # no cdp run
SecureRoute1 (config) # exit
SecureRoute1# show cdp
% CDP is not enabled
SecureRoute1#

Vulnerability Comparison by machine with solutions

Vulnerability Name Default private SNMP community is configured.

Vulnerability Description :

A default or unprotected community name of "private" was discovered. An attacker can use this to gather information from the vulnerable device that is very useful in mounting a more sophisticated attack.

Solution :

It is recommended to disable the SNMP if it is not a business requirement by using the commands shown below in global configuration mode.

```
SecureRoute1 # config t
Enter configuration commands, one per line. End with
CNTL/Z.
SecureRoute1 # ! In order to disable SNMP Server
SecureRoute1 # no snmp-server
SNMP disabled.
SecureRoute1 # (enable)
In order to verify the SNMP configuration type:
SecureRoute1 # show snmp
Create an access list of permitted SNMP stations
SecureRoute1 # set snmp access-list 2 10.2.60.100 mask
255.255.255.0
If read only SNMP is used, change the community string
SecureRoute1 # set snmp-server community read-only
53cur5nmp
In order to remove public community string
SecureRoute1 # no snmp-server community public RO

If read/write SNMP is used, change the community string
SecureRoute1 # set snmp-server community read-write
53cur7Yuhs
In order to remove private community string
SecureRoute1 # no snmp-server community private RO
```

Vulnerability Name Default public SNMP community is configured.

Vulnerability Description :

Solution :



Vulnerability Comparison by machine with solutions

A default or unprotected community name of "public" was discovered. An attacker can use this to gather information from the vulnerable device that is very useful in mounting a more sophisticated attack.

It is recommended to disable the SNMP if it is not a business requirement by using the commands shown below in global configuration mode.

```
SecureRoute1 # config t
Enter configuration commands, one per line. End with
CNTL/Z.
SecureRoute1 # ! In order to disable SNMP Server
SecureRoute1 # no snmp-server
SNMP disabled.
SecureRoute1 # (enable)
In order to verify the SNMP configuration type:
SecureRoute1 # show snmp
Create an access list of permitted SNMP stations
SecureRoute1 # set snmp access-list 2 10.2.60.100 mask
255.255.255.0
If read only SNMP is used, change the community string
SecureRoute1 # set snmp-server community read-only
53cur5nmp
In order to remove public community string
SecureRoute1 # no snmp-server community public RO
If read/write SNMP is used, change the community string
SecureRoute1 # set snmp-server community read-write
53cur7Yuhs
In order to remove private community string
SecureRoute1 # no snmp-server community private RO
```

Vulnerability Name HTTP Server is configured.

Vulnerability Description :

On this router http server is running with web-based remote administration. While the web access features are fairly rudimentary on most Cisco router IOS releases, they are a viable mechanism for monitoring, configuring, and attacking a router. It is recommended not to use http server.

Solution :

```
In order to disable HTTP Server
Securerouter1 # config t
Enter configuration commands, one per line. End with
CNTL/Z.
Securerouter1 (config) # no ip http server
Securerouter1 (config) # exit
```

Vulnerability Name IP BOOTP Server Service is enabled.

Vulnerability Description :

This service allows other routers to boot from this router. This service is not in use and IT experts recommend not to use this service, so disable it. It is possible it may open a security hole. In order to disable this service use this command.

Solution :

```
In order to disable the IP BOOTP Server.
Securerouter1 # config t
Enter configuration commands, one per line. End with
CNTL/Z.
Securerouter1 (config) # no ip bootp server
Securerouter1 (config) # exit
```

Vulnerability Name Minimum Password Length is not configured.

Vulnerability Comparison by machine with solutions

Vulnerability Description :

This route is not configure with Minimum Password Length this should be set in order to enforce the company policy and protect against brute force attack. It is recommended to set this value to 6 or according to the company policy.

Solution :

In Order to set security passwords min-length
Securerouter1# config t
Enter configuration commands, one per line. End with CNTL/Z.
Securerouter1 (config) # security passwords min-length <6>
Securerouter1 (config) # exit

Vulnerability Name Network Time Protocol (NTP) is enabled.

Vulnerability Description :

By default, a Cisco router configured with one or more NTP servers or peers will act as an NTP server. Unless your network is responsible for providing time service to other networks, Secure Bytes recommend that NTP should be disable on all external interfaces.

Solution :

In order to mitigate this vulnerability one should disable NTP, using the commands shown below in global configuration mode.
SecureRoute1 # config t
Enter configuration commands, one per line. End with CNTL/Z.
SecureRoute1 (config) # NTP disable
SecureRoute1 (config) # exit

Vulnerability Name Privilege level is not set for user accounts.

Vulnerability Description :

Ensure all user accounts are assigned the lowest privilege level that allows them to perform their duties. By not restricting administrators and operations personnel to their proper privilege levels, access to restricted functions may be allowed before they are trained or experienced enough to use those functions. Network disruptions or outages could be caused by mistakes made by inexperienced administrators

Solution :

The administrator will assign accounts with the least privilege rule. Each user will have access to only the privileges they require to perform their respective duties. Access to the highest privilege levels should be restricted to a few users.
There would be several username name password password followed by username name privilege level. The user will automatically be granted that privilege level upon logging in. Below is an example of assigning a privilege level to a local user account and changing the default privilege levels of the configure terminal command.
Secureswitch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Secureswitch# username junior-engineer1 privilege 7 password xxxxxx
Secureswitch# privilege exec level 7 configure terminal
Secureswitch# exit
Secureswitch# write memory

Vulnerability Name Rip Version 1 is configured on the device.

Vulnerability Description :

Solution :

Vulnerability Comparison by machine with solutions

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. There are two versions of the Routing Information Protocol available on Cisco devices: RIP Version 1 and RIP Version 2. By default, the software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets. You can configure the software to receive and send only Version 1 packets. Alternatively, you can configure the software to receive and send only Version 2 packets. Cisco's implementation of RIP Version 2 supports authentication, key management, route summarization, classless inter domain routing (CIDR), and variable-length subnet masks (VLSMs). Key management and VLSM are described in the chapter "Configuring IP Routing Protocol-Independent Features." That is the why it is recommended that one should RIP Version 2.

In order to configure RIP Version 2 use the following command in router configuration mode:
 Securerouter1 # config t
 Enter configuration commands, one per line. End with CNTL/Z.
 Securerouter1 (config) # router RIP
 Securerouter1 (config) #version 2
 Securerouter1 (config) # exit
 Securerouter1 # write memory

Vulnerability Name Secure Copy (SCP) is not enabled.

Vulnerability Description :

The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files. SCP relies on Secure Shell (SSH). Because SCP relies on SSH for its secure transport, the router must have an RSA key pair, SSH must be configured and enabled on the router and Authentication and authorization must be configured correctly to enable SCP.

Solution :

SSH must be configured and functioning properly.
 SecureRoute1 # config t
 Enter configuration commands, one per line. End with CNTL/Z.
 SecureRoute1 (config) # ip ssh time-out 120
 SecureRoute1 (config) # ip ssh authentication-retries 3
 SecureRoute1 (config) # ip scp server enable

Vulnerability Name TCP Synwait Time is not configured.

Vulnerability Description :

In order to help prevent the SYN Flood attack the administrator can set the amount of time the switch will wait while attempting to establish a TCP connection. The following command sets the wait time to 10 seconds.

Solution :

In Order to enable TCP Synwait Time
 The following command sets the wait time to 10 seconds.
 Securerouter1 # config t
 Enter configuration commands, one per line. End with CNTL/Z.
 Securerouter1 (config) # ip tcp synwait-time 10
 Securerouter1 (config) # exit

Vulnerability Name The Simple Network Management Protocol (SNMP) is enabled.

Vulnerability Description :

Solution :



Vulnerability Comparison by machine with solutions

Loopback interfaces are virtual interfaces that are always up. This feature has many benefits, especially when you use routing protocols that use active interfaces as part of their configuration protocol, such as OSPF. You can also use the loopback interface IP address as the source address for traffic generated by the device. Thus, defining a single loopback interface per device can enhance overall network stability and security. You can also use ACLs to further protect access to the device using the loopback interface's address.

```
IOS (config)#snmp-server trap-source
Loopback<Loopback number>
Step By Step for IOS
hostname # config t
Enter configuration commands, one per line. End with
CNTL/Z.
hostname (config)# snmp-server trap-source Loopback
0
hostname (config)# exit
hostname (config)#
```

Audit Performed:	CiscoAudit(Sep 27 2011 2:55PM)	Selected Profile:	SCA
Machine :	192.168.68.203		
Risk Level :	Informational		

Vulnerability Name Cisco IOS Version.

Vulnerability Description :

The IOS image running on a router determines the features, capabilities and initial configuration settings that need locking down. The various IOS software images support different protocols and features and have different configuration requirements.

Solution :

This is only for information, there is no quick fix in order to find out what version of IOS to upgrade to, visit Ciscos online Software Planner at <http://www.cisco.com/kobayashi/sw-center/>. This requires a Cisco Connection Online (CCO) account.

Vulnerability Name Cisco show route.

Vulnerability Description :

This is only for information showing routing information on the device. It helps the administrator in troubleshooting the device.

Solution :

This is only for information; there is no quick fix for it. For adding a static route
 config term
 ip route 10.10.20.0 255.255.255.0 192.168.100.1
 For adding a default route
 ip route 0.0.0.0 0.0.0.0 38.167.29.1
 PIX, ASA, FWSM (config) #no http server enable

Vulnerability Name The Configuration Register is set.

Vulnerability Description :

This tells the router how to boot and to change the configuration register setting and it also helps in recovery of the password.

Solution :

This is for information only. If the router's configuration register is not set to 0x2102, record the current value, and use the following commands to set it to the required value:
 SecureRouter# configure terminal
 secureRouter(config)# config-reg 0x2102
 secureRouter(config)# exit
 securerouter#reload