secure auditor

Audit Report

Vulnerability categorization by machine

Report Generated Time: 9/27/2011 At 2:59:53PM

Audit Name: : CiscoAudit(Sep 27 2011 2:55PM)
Description: : Cisco Audit Report
IP Count : 1
IPs: : 192.168.68.203

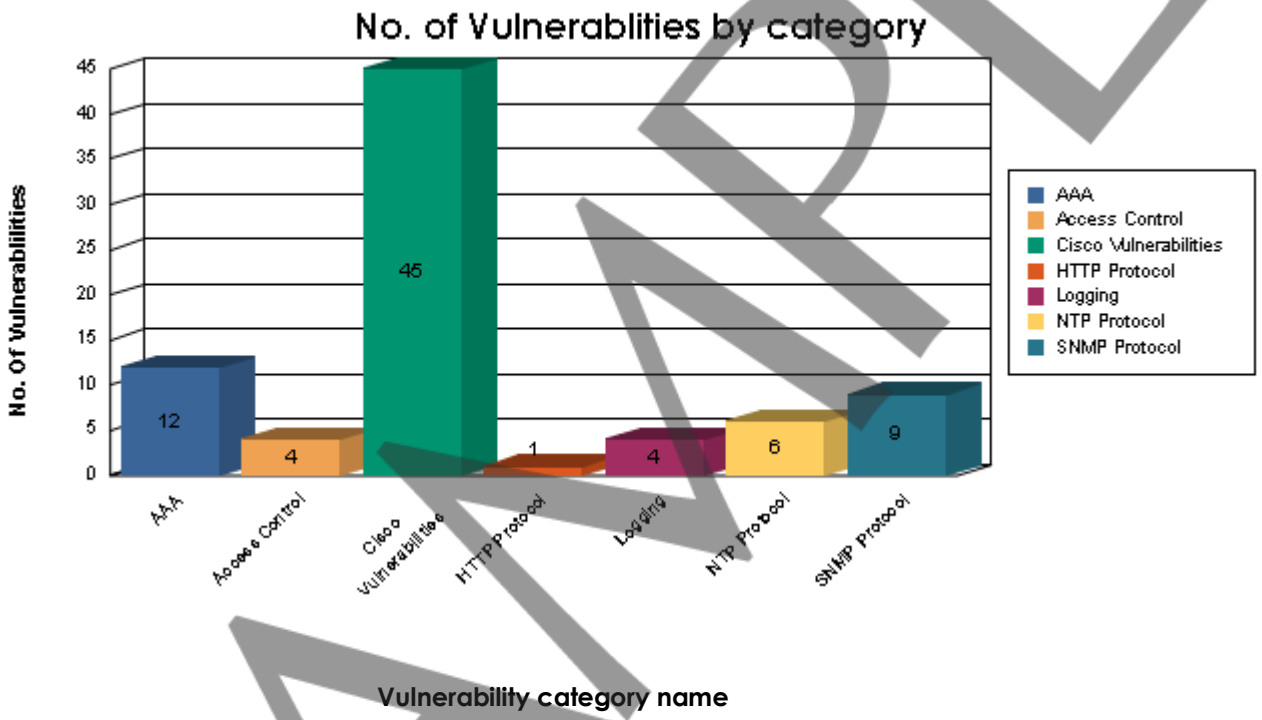
Licensed To : Support
Company Name : Secure Bytes

SECURE BYTES

Vulnerability categorization by machine

Report generated on 27-Sep-2011 at 2:59:53PM

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.



Vulnerability categorization by machine

Category	**AAA**		
Audit Performed :	**CiscoAudit(Sep 27 2011 2:55PM)**	**Selected Profile:**	**SCA**
Machine IP	**192.168.68.203**	**Machine Port :**	**22**
	Detail		
Risk Level :	Medium		
Name	AAA Accounting commands is not configured.		
Description	It is very help full for administrator , he can watch any user that which commands did he run.		
Risk Level :	Medium		
Name	AAA Accounting connection is not configured		
Description	aaa accounting connection is very helpful if someone connect to other device form that router then that will be log and administrator can easily detect the malicious attack.		
Risk Level :	Medium		
Name	AAA Accounting exec is not configured.		
Description	It is very important command for tracking purposes , for example if a user did a malicious activity then how to catch him? The radius or tacscs server has all information about user activities that is helpful for catching attacker.		
Risk Level :	Medium		
Name	AAA Accounting network is not configured.		
Description	It is another helpful command use to detect the attacker .		
Risk Level :	Medium		
Name	AAA Accounting system is not configured.		
Description	It gives the information about rebooting or router and which user did that. Reboot of routre is a dangerous attack if some one did it remotely without permission.		
Risk Level :	Medium		
Name	AAA Authentication enable is not configured.		
Description	Authentication is the mechanism for identifying users before allowing access to network components or services. In other words, authentication controls the ability of a user or another network component to access a network device or service. AAA authentication provides the means for identifying users through login/password dialogs, challenge/response mechanisms, and supported token technologies. Although authentication can be configured without using AAA, to use security server protocols or backup authentication methods you must use AAA authentication. For AAA authentication the available methods are RADIUS, TACACS+, Kerberos, local username database, line passwords, enable passwords and none.		
Risk Level :	Medium		
Name	AAA Authentication is not enabled on Console and VTY Lines		

Vulnerability categorization by machine

Description	The required AAA authentication method list is used for logins on the selected line types. If you are using AAA authentication in your network, using AAA authentication for line access to the network devices enhances security and provides better centralized control of your network.
Risk Level :	Medium
Name	AAA Authentication login is not configured.
Description	The AAA security services facilitate a variety of login authentication methods.
Risk Level :	Medium
Name	AAA Authorization command is not configured.
Description	aaa authorization commands used to restrict the user from executing commands like conf t. In order to restrict user then use that command.
Risk Level :	Medium
Name	AAA Authorization exec is not configured.
Description	Authorization controls access to system resources.If aaa authorization is not set then an unauthorized user but only authenticated users can access the router console and can execute each and every command.
Risk Level :	Medium
Name	AAA Authorization network is not configured.
Description	aaa authorization network enables authorization for all network related services like: PPP, PPP NCP's, SLIP, and ARA Protocols.
Risk Level :	Medium
Name	AAA Authorization reverse-access is not configured.
Description	If aaa authorization reverse-access not set then a authenticated user can run the reverse telnet service and connect to router and router will be fully control by that person. In order to restrict user from using that service then apply that authorization to secure youre router .
12	**Vulnerability/ies of type AAA**
Category	**Access Control**
Audit Performed :	**CiscoAudit(Sep 27 2011 2:55PM)** **Selected Profile: SCA**
Machine IP	**192.168.68.203** **Machine Port : 22**
	Detail
Risk Level :	High
Name	Authentication Retry settings are not configuration for SSH
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.
Risk Level :	Medium
Name	Control plane protection is not enabled on the router or multilayer switch only.

Vulnerability categorization by machine

Description

The Route Processor (RP) is critical to all network operations as it is the component used to build all forwarding paths for the data plane via control plane processes. It is also instrumental with ongoing network management functions that keep the routers and links available for providing network services. Hence, any disruption to the RP or the control and management planes can result in mission critical network outages.
In addition to control plane and management plane traffic that is in the router's receive path, the RP must also handle other traffic that must be punted to the RP—that is, the traffic must be fast or process switched. This is the result of packets that must be fragmented, require an ICMP response (TTL expiration, unreachable, etc.) have IP options, etc. A DoS attack targeting the RP can be perpetrated either inadvertently or maliciously involves high rates of punted traffic resulting in excessive RP CPU and memory utilization. To maintain network stability, the router must be able to securely handle specific control plane and management plane traffic that is destined to it as well as other punted traffic.
Using the ingress filter on forwarding interfaces is a method that has been used in the past to filter both forwarding path and receive path traffic. However, this method does not scale well as the number of interfaces grows and the size of the ingress filters grow. Control plane policing can be used to increase security of routers and multilayer switches by protecting the RP from unnecessary or malicious traffic. Filtering and rate limiting the traffic flow of control plane packets can be implemented to protect routers against reconnaissance and DoS attacks allowing the control plane to maintain packet forwarding and protocol states despite an attack or heavy load on the router or multilayer switch.

Risk Level :	Medium
Name	Timeout for Login Sessions is not set for SSH.
Description	This prevents unauthorized users from misusing abandoned sessions. Example, if the administrator leaves an enabled login session active on his desktop system. There is a trade-off here between security (shorter timeouts) and usability (longer timeouts). Check your local policies and operational needs to determine the best value. In most cases, this should be no more than 10 minutes.
Risk Level :	Informational
Name	Cisco show route.
Description	This is only for information showing routing information on the device. It helps the administrator in troubleshooting the device.

4	**Vulnerability/ies of type Access Control**		
Category	**Cisco Vulnerabilities**		
Audit Performed :	**CiscoAudit(Sep 27 2011 2:55PM)**	**Selected Profile:**	**SCA**
Machine IP	**192.168.68.203**	**Machine Port :**	**22**

Detail

Risk Level :	High
Name	Access Class is not configured on VTY.
Description	On cicso 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.

Vulnerability categorization by machine

Risk Level :	High
Name	Cisco Discovery Protocol (CDP) is enabled.
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.
Risk Level :	High
Name	IP BOOTP Server Service is enabled.
Description	This service allow other routers to boot from this router mostly service is not in used and IT Experts recomend not to use this service, so disable it, It is possible it may open a security hole. In order to disable this service us this command.
Risk Level :	High
Name	Minimum Password Length is not configured.
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.
Risk Level :	High
Name	Privilege level is not set for user accounts.
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
Risk Level :	High
Name	Rip Version 1 is configured on the device.
Description	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.
Risk Level :	High
Name	Secure Copy (SCP) is not enabled.

Vulnerability categorization by machine

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.
Risk Level :	High
Name	TCP Synwait Time is not configured.
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.
Risk Level :	High
Name	Too many virtual terminals are configured.
Description	Most versions of IOS have five virtual terminals, numbered 0 through 4. Some IOS versions may have 15, 64, or even more. It is important to know how many virtual terminals your IOS version has, and to explicitly configure all of them securely.
Risk Level :	High
Name	Trivial File Transfer Protocol (TFTP) is enabled.
Description	The Trivial File Transfer Protocol (TFTP) is a UDP based protocol which provides file transfers without any authentication or security therefore Secure Bytes does not recommend it's use. Instead use SCP or FTP, however if this is a business requirement It can be configured.
Risk Level :	High
Name	Unicast RPF is enabled on required Interface.
Description	Most Cisco routers running IOS 12.0 and later support a routing-based filtering feature called IP unicast reverse-path forward (Unicast RPF) verification. When this feature is enabled on an interface, the router uses its routing tables to decide whether to accept or drop individual packets arriving on the interface. It is good security practice to reject a packet with a spoofed source address. Unicast reverse-path verification supports rejecting such packets, and in some cases it can offer significant advantages over using access lists for that purpose. Unicast reverse-path verification is not enabled by default; you must explicitly apply it to each interface where you want verification to be done. Used correctly, and in situations where it applies, unicast RPF verification prevents most forms of IP address spoofing.
Risk Level :	High
Name	User-based HTTP Authentication not configured.
Description	When the HTTP service is running on a device, the default authorization password is the device's enable password, and the user name is ignored. To strengthen user authorization, you should enable user-based authentication for HTTP access. This requires each user to have a valid user name and password to access the device through a web browser.
Risk Level :	High
Name	VTY exec-timeout is not configured.
Description	To set the interval that the EXEC command interpreter waits until user input is detected, use the exec-timeout command in line configuration mode.

Vulnerability categorization by machine

Risk Level :	Medium
Name	SNMP Traps should be disabled.
Description	SNMP should be disabled unless you absolutely require them for network management purposes.
Risk Level :	Medium
Name	SNMP Write Access should be disabled.
Description	SNMP Write access allows remote monitoring change configration and management of the device. Older version of the protocol, such as SNMP versions 1 and 2, do not use any encryption to protect community strings (passwords). SNMP should be disabled unless you absolutely require it for network management purposes. If you require SNMP, be sure to select SNMP community strings that are strong passwords, and are not the same as other passwords used for the device (e.g. enable password, line password, etc.) or other authentication credentials. Consider utilizing SNMPv3 which utilizes authentication and data privatization (encryption), when available. SNMP versions 1 and 2 use clear-text community strings, which are considered a weak security implementation.
Risk Level :	Medium
Name	Trap Service is not bind to Loopback Interface.
Description	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.

9	**Vulnerability/ies of type SNMP Protocol**
Total Vulnerabilities:	**81**