



secure auditor

Audit Report

Vulnerability Details and Their Solutions

Report Generated Time: 9/27/2011 At 2:55:37PM

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

Description: : Cisco Audit Report

IP Count : 1

IP(s): : 192.168.68.203

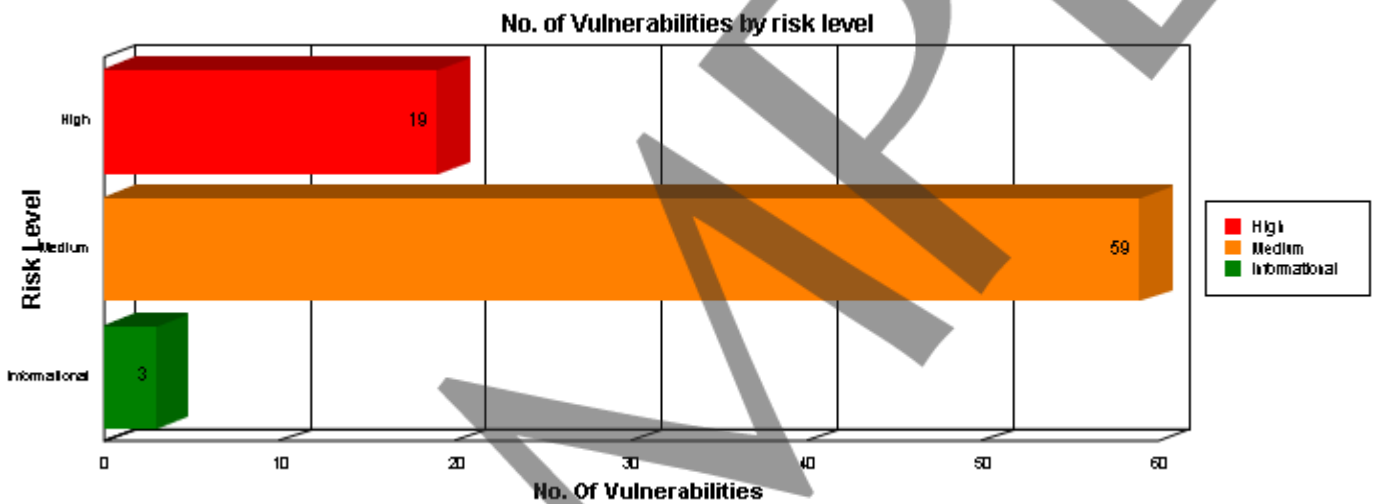




Vulnerability Details and Their Solutions

Report generated on 27-Sep-2011 At 2:55:37PM

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 posture. 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



Vulnerability details and their solutions

Summary Information :

Machine : 192.168.68.203		Selected Profile: SCA
Risk Level	Number of Vulnerabilities	Percentage
High	19	23.46%
Medium	59	72.84%
Informational	3	3.70%
Vulnerabilities on 192.168.68.203	81	100.00%
Total Vulnerabilities:	81	100.00%

SAMPLE



Vulnerability details and their solutions

Machine	192.168.68.203
Risk Level	High
Selected Profile: SCA	

Vulnerability: Access Class is not configured on VTY.

Vulnerability's Occurrence::	1	Machine	192.168.68.203	Port:	22
Risk Level	High	Product Name	Cisco	Vendor	Cisco
Versions	All IOS Versions	Test Type Name	Audit		

Vulnerability Information:

Category Name Cisco Vulnerabilities

Overview: One primary mechanism for remote administration of Cisco routers is logging in via Telnet; these connections are called virtual terminal lines. Login on the virtual terminal lines should be disabled if remote administration is not absolutely necessary. Remote administration is inherently dangerous because anyone with a network sniffer on the right LAN segment can acquire the router passwords and would then be able to take control of the router. To disable network virtual terminal connections to the router, create an access list and apply it to the virtual terminal lines.

Vulnerability References:

References http://www.cisco.com/en/US/products/products_security_advisory09186a00802acbf6.shtml

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 Specifications: :

access-class is not configured



Vulnerability details and their solutions

Vulnerability: Authentication Retry settings are not configuration for SSH

Vulnerability's Occurrence::	1	Machine	192.168.68.203	Port:	22
Risk Level	High	Product Name	Cisco	Vendor	Cisco
Versions	Cisco IOS 12 and above	Test Type Name	Audit		

Vulnerability Information:

Category Name Access Control

Overview: Authentication Retry settings are not configuration for SSH

Vulnerability References:

References http://www.cisecurity.org/tools2/cisco/CIS_Cisco_IOS_Benchmark_v2.2.pdf
http://www.cisecurity.org/tools2/cisco/CIS_Cisco_Firewall_Benchmark_v2.0.pdf
http://www.nsa.gov/ia/guidance/security_configuration_guides/current_guides.shtml

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 Specifications: :

ip ssh authentication-retries is not configured



Vulnerability details and their solutions

Vulnerability: Cisco Discovery Protocol (CDP) is enabled.

Vulnerability's Occurrence::	1	Machine	192.168.68.203	Port:	22
Risk Level	High	Product Name	Cisco	Vendor	Cisco
Versions	All IOS Versions	Test Type Name	Audit		

Vulnerability Information:

Category Name Cisco Vulnerabilities

Overview: The Cisco Discovery Protocol is a proprietary protocol that Cisco routers use to identify each other on a LAN segment. It is useful only in specialized situations, and is considered deleterious to security. To disable the automatic loading of configuration files from a network server turn off the service configuration. This service does not depend upon any type of authentication or confirmation regarding the validity of the data stream that it receives from the service. This makes this service potentially susceptible to compromising the configuration of the router.

Vulnerability References:

References http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#cdp

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 Specifications:

cdp is not enabled is not configured



Vulnerability details and their solutions

Vulnerability: **Default private SNMP community is configured.**

Vulnerability's Occurrence::	1	Machine	192.168.68.203	Port:	22
Risk Level	High	Product Name	Cisco	Vendor	Cisco
Versions	All IOS Versions	Test Type Name	Audit		

Vulnerability Information:

Category Name SNMP Protocol

Overview: SNMP is a vulnerable service to use on an internetwork and should be used with Caution. Many devices have community strings (which are SNMP passwords) public for read-only access and private for read-write access. An SNMP sweep should be done of the routers on the internetwork. If either public or private is found, they should be removed immediately and replaced with strong passwords. Multiple versions of SNMP are available: SNMPv1, SNMPv2c, and SNMPv3. SNMPv3 provides several important security features: message integrity, authentication and encryption. SNMPv3 uses HMAC-MD5 or HMAC-SHA for authentication and 56-bit DES for encryption. If possible, use a different MD5 secret value for sections of the network or for each router. If SNMP is not required then it should be removed. If it is an operational requirement then use SNMPv3.

Vulnerability References:

References http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa4.shtml#enablesnmp

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 recommends to disable the SNMP If it is not a business requirement by using this 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 Specifications: :

snmp-server community private rw

Vulnerability details and their solutions

showversionCisco IOS Software, 1841 Software (C1841-ADVSECURITYK9-M), Version 12.4(19), RELEASE SOFTWARE (fc1)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 29-Feb-08 18:26 by prod_rel_team

ROM: System Bootstrap, Version 12.3(8r)T9, RELEASE SOFTWARE (fc1)

Router3 uptime is 5 hours, 3 minutes
System returned to ROM by power-on
System image file is "flash:c1841-advsecurityk9-mz.124-19.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/www/export/crypto/tool/starg.html>
If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 1841 (revision 6.0) with 115712K/15360K bytes of memory.
Processor board ID FCZ102610VV
2 FastEthernet interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

Router3#
