172.26.0.50

1 Result

IOS System Diagnostics

Diagnostic Checks: **2460**

Apr 16th 2020 9:30:31 pm (4 days ago)

 7 Info

Restrict SNMP community access with ACL as a security best practice

When defining the SNMP community, an ACL should be applied to restricts SNMP access to a select group of source IP addresses as a security best practice.   
For details please refer to: <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc53>

snmp-server community <removed> RO

SNMP is enabled but not running version 3, which is a security best practice

SNMP is enabled but not running SNMP version 3 (SNMPv3). SNMPv3 provides secure network management access to devices by authenticating and optionally encrypting management data packets over the network, thereby protecting the device from potential security exploits.   
For details please refer to: <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc56>

snmp-server community <removed> RO

Found missing router security best practices

The following router security best practices are missing on this device. These are highly recommended configurations to help improve the security posture of the device:

 Login Dictionary Attack Protection - to deny aditional connections after a failed number of login attempts, see <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xe-3s/sec-usr-cfg-xe-3s-book/sec-login-enhance.html#GUID-270568E3-5BA8-4781-8988-707BF91CC427>

 Enable Keepalives For TCP Sessions - to help avoid hung management TCP sessions, see <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc19>

 Enable NTP Authentication - to ensure the NTP time source is trusted, see <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc27>

IP Source Routing is enabled, which is a deviation from the router security hardening best practices

The IP source routing options allows the sender of an IP packet to control the route that the datagram will take toward its ultimate destination, and generally the route that any reply will take. This feature is enabled by default with the commad **ip source-route**. This service is usually not needed and should be disabled to improve the security posture of the device.  
  
For more information please see Network Security Baseline: <http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/sec_chap4.html#wp1056514>.

Syslog entries found in show logging (severity warning or higher)

There has been 1 unique Syslog entry found in the "show logging" (severity warning or higher).  
  
---------------------------------------------------  
| Syslog with Severity level **Warnings**  
---------------------------------------------------  
**Error message** (Seen **1** time, the most recent at **Apr 16 15:52:47.138**):  
SSH-4-SSH2\_UNEXPECTED\_MSG: Unexpected message type has arrived. Terminating the connection  
**Explanation**:  
SSH Session closure warning on receiving an inappropriate message from the peer  
**Recommended Action**:  
These error messages are usually caused by a client doing an ssh-keyscan or by the client using the wrong RSA key.  
a) On the device, run: # show ip ssh  
b) On the client, look at the key for the SWITCH\_IP in ~/.ssh/known\_hosts or wherever else it is stored.  
c) Compare the keys. If the keys don't match, re-generate key on the client.

.Apr 16 15:52:47.138: %SSH-4-SSH2\_UNEXPECTED\_MSG: Unexpected message type has arrived. Terminating the connection

The device's clock may be incorrect

The device has an authoritative time but is no longer synced with NTP. The time on the device is considered valid and will allow functions like PKI to operate however without continued syncing with an NTP server the time on this device may skew and cause problems with time sensitive applications. See the following link for more information: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/xe-3s/bsm-xe-3s-book/bsm-time-calendar-set.html#GUID-25ECF2C2-3801-4A93-AF49-851FB3ED9799>

.21:27:03.308 IST Thu Apr 16 2020

The data from this device (FOC1726Z1M9) was evaluated against 2460 different diagnostic checks .