STIG Findings

# Finding Table

|  |  |
| --- | --- |
| Rule ID | Finding |
| V-215807 | FAIL |
| V-215813 | FAIL |
| V-215814 | FAIL |
| V-215815 | FAIL |
| V-215816 | FAIL |
| V-215817 | FAIL |
| V-215820 | FAIL |
| V-215823 | PASS |
| V-215825 | FAIL |
| V-215832 | FAIL |
| V-215833 | PASS |
| V-215836 | FAIL |
| V-215840 | FAIL |
| V-215844 | FAIL |
| V-215845 | FAIL |
| V-216675 | PASS |
| V-216700 | FAIL |
| V-216726 | FAIL |
| V-216727 | FAIL |
| V-217001 | FAIL |
| V-215808 | FAIL |
| V-215809 | FAIL |
| V-215810 | FAIL |
| V-215811 | FAIL |
| V-215819 | FAIL |
| V-215821 | FAIL |
| V-215822 | FAIL |
| V-215834 | FAIL |
| V-215835 | FAIL |
| V-215839 | FAIL |
| V-215847 | FAIL |
| V-215848 | FAIL |
| V-215849 | FAIL |
| V-215850 | FAIL |
| V-215852 | FAIL |
| V-216647 | PASS |

# V-215807

The Cisco router must be configured to limit the number of concurrent management sessions to an organization-defined number.

Finding on device: **FAIL**

Rule Title: SRG-APP-000001-NDM-000200

Rule Severity: medium

Suggested Fix:

Configure the router to limit the number of concurrent management sessions to an organization-defined number as shown in the example below.  
  
ip http max-connections 2  
line vty 0 4  
 session-limit 2

# V-215813

The Cisco router must be configured to enforce the limit of three consecutive invalid logon attempts, after which time it must lock out the user account from accessing the device for 15 minutes.

Finding on device: **FAIL**

Rule Title: SRG-APP-000065-NDM-000214

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to enforce the limit of three consecutive invalid logon attempts as shown in the example below.  
  
R2(config)#login block-for 900 attempts 3 within 120

# V-215814

The Cisco router must be configured to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the device.

Finding on device: **FAIL**

Rule Title: SRG-APP-000068-NDM-000215

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to display the Standard Mandatory DoD Notice and Consent Banner before granting access as shown in the following example:  
  
R1(config)#banner login #  
Enter TEXT message. End with the character '#'.  
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. #  
R1(config)#end

# V-215815

The Cisco router must be configured to protect against an individual falsely denying having performed organization-defined actions to be covered by non-repudiation.

Finding on device: **FAIL**

Rule Title: SRG-APP-000080-NDM-000220

Rule Severity: medium

Suggested Fix:

Configure the router to log administrator activity as shown in the example below.  
  
R1(config)#logging userinfo  
R1(config)#archive  
R1(config-archive)#log config  
R1(config-archive-log-cfg)#logging enable  
R1(config-archive-log-cfg)#end

# V-215816

The Cisco router must be configured to generate audit records when successful/unsuccessful attempts to log on with access privileges occur.

Finding on device: **FAIL**

Rule Title: SRG-APP-000091-NDM-000223

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to log all logon attempts as shown in the example below.  
  
R1(config)#login on-failure log  
R1(config)#login on-success log  
R1(config)#end

# V-215817

The Cisco router must produce audit records containing information to establish when (date and time) the events occurred.

Finding on device: **FAIL**

Rule Title: SRG-APP-000096-NDM-000226

Rule Severity: medium

Suggested Fix:

Configure the router to include the date and time on all log records as shown in the example below.  
  
R1(config)#service timestamps log datetime localtime

# V-215820

The Cisco router must be configured to protect audit information from unauthorized modification.

Finding on device: **FAIL**

Rule Title: SRG-APP-000119-NDM-000236

Rule Severity: medium

Suggested Fix:

If persistent logging is enabled, configure the router to only allow administrators with privilege level "15" access to the file system as shown in the example below.  
  
R4(config)#file privilege 15

# V-215823

The Cisco router must be configured to prohibit the use of all unnecessary and nonsecure functions and services.

Finding on device: **PASS**

Rule Title: SRG-APP-000142-NDM-000245

Rule Severity: high

# V-215825

The Cisco router must be configured to implement replay-resistant authentication mechanisms for network access to privileged accounts.

Finding on device: **FAIL**

Rule Title: SRG-APP-000156-NDM-000250

Rule Severity: medium

Suggested Fix:

Configure SSH to use FIPS-140-2 compliant HMACs as shown in the example below.  
  
R1(config)#ip ssh version 2  
R1(config)#ip ssh server algorithm encryption aes128-cbc aes192-cbc aes192-ctr  
  
Note: An SSH configuration enables a server and client to authorize the negotiation of only those algorithms that are configured from the allowed list. If a user tries to negotiate using an algorithm that is not part of the allowed list, the request is rejected and the session is not established.

# V-215832

The Cisco router must only store cryptographic representations of passwords.

Finding on device: **FAIL**

Rule Title: SRG-APP-000171-NDM-000258

Rule Severity: high

Suggested Fix:

Configure the router to encrypt all passwords.  
  
R4(config)#service password-encryption   
R4(config)#end

# V-215833

The Cisco router must be configured to terminate all network connections associated with device management after 10 minutes of inactivity.

Finding on device: **PASS**

Rule Title: SRG-APP-000190-NDM-000267

Rule Severity: high

# V-215836

The Cisco router must be configured to allocate audit record storage capacity in accordance with organization-defined audit record storage requirements.

Finding on device: **FAIL**

Rule Title: SRG-APP-000357-NDM-000293

Rule Severity: medium

Suggested Fix:

Configure the buffer size for logging as shown in the example below.  
  
R2(config)#logging buffered xxxxxxxx informational

# V-215840

The Cisco router must be configured to record time stamps for log records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

Finding on device: **FAIL**

Rule Title: SRG-APP-000374-NDM-000299

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to record time stamps for audit records that can be mapped to UTC or GMT as shown in the example below.  
  
R2(config)#clock timezone EST -5  
R2(config)#service timestamps log datetime localtime

# V-215844

The Cisco router must be configured to use FIPS-validated Keyed-Hash Message Authentication Code (HMAC) to protect the integrity of remote maintenance sessions.

Finding on device: **FAIL**

Rule Title: SRG-APP-000411-NDM-000330

Rule Severity: high

Suggested Fix:

The Cisco router is not compliant with this requirement. However, the risk associated with this requirement can be fully mitigated if the router is configured.  
  
Configure SSH and HTTPs to use FIPS-validated HMAC for remote maintenance sessions as shown in the following examples:  
  
SSH Example  
  
R1(config)#ip ssh version 2  
R1(config)#ip ssh server algorithm mac hmac-sha1-96  
  
HTTPS Example  
  
R2(config)#ip http secure-ciphersuite aes-128-cbc-sha

# V-215845

The Cisco router must be configured to implement cryptographic mechanisms to protect the confidentiality of remote maintenance sessions.

Finding on device: **FAIL**

Rule Title: SRG-APP-000412-NDM-000331

Rule Severity: high

Suggested Fix:

Configure the Cisco router to implement cryptographic mechanisms to protect the confidentiality of remote maintenance sessions using a FIPS 140-2 approved algorithm as shown in the examples below.  
  
SSH Example  
  
R1(config)#ip ssh server algorithm encryption aes128-cbc aes128-ctr aes192-cbc aes192-ctr  
  
HTTPS Example  
  
R2(config)#ip http secure-ciphersuite aes-128-cbc-sha

# V-216675

The Cisco perimeter router must be configured to have Cisco Discovery Protocol (CDP) disabled on all external interfaces.

Finding on device: **PASS**

Rule Title: SRG-NET-000364-RTR-000111

Rule Severity: low

# V-216700

The Cisco MPLS router must be configured to have TTL Propagation disabled.

Finding on device: **FAIL**

Rule Title: SRG-NET-000512-RTR-000004

Rule Severity: medium

Suggested Fix:

Configure the MPLS router to disable TTL propagation as shown in the example below:  
  
R5(config)#no mpls ip propagate-ttl

# V-216726

The Cisco multicast Designated Router (DR) must be configured to limit the number of mroute states resulting from Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Host Membership Reports.

Finding on device: **FAIL**

Rule Title: SRG-NET-000362-RTR-000122

Rule Severity: medium

Suggested Fix:

Configure the DR on a global or interface basis to limit the number of mroute states resulting from IGMP or MLD membership reports.  
  
R3(config)#int g0/0  
R3(config-if)#ip igmp limit 2

# V-216727

The Cisco multicast Designated Router (DR) must be configured to set the shortest-path tree (SPT) threshold to infinity to minimalize source-group (S, G) state within the multicast topology where Any Source Multicast (ASM) is deployed.

Finding on device: **FAIL**

Rule Title: SRG-NET-000362-RTR-000123

Rule Severity: medium

Suggested Fix:

Configure the DR to increase the SPT threshold or set it to infinity to minimalize (S, G) state within the multicast topology where ASM is deployed.  
  
R3(config)#ip pim spt-threshold infinity

# V-217001

The Cisco PE router must be configured to ignore or drop all packets with any IP options.

Finding on device: **FAIL**

Rule Title: SRG-NET-000205-RTR-000016

Rule Severity: medium

Suggested Fix:

Configure the router to ignore or drop all packets with IP options as shown in the examples below:  
  
R4(config)#ip options ignore   
  
or  
  
R4(config)#ip options drop

# V-215808

The Cisco router must be configured to automatically audit account creation.

Finding on device: **FAIL**

Rule Title: SRG-APP-000026-NDM-000208

Rule Severity: medium

Suggested Fix:

Configure the router to log account creation using the following commands:  
  
R4(config)#archive  
R4(config-archive)#log config  
R4(config-archive-log-cfg)#logging enable  
R4(config-archive-log-cfg)#end

# V-215809

The Cisco router must be configured to automatically audit account modification.

Finding on device: **FAIL**

Rule Title: SRG-APP-000027-NDM-000209

Rule Severity: medium

Suggested Fix:

Configure the router to log account modification using the following commands:  
  
R4(config)#archive  
R4(config-archive)#log config  
R4(config-archive-log-cfg)#logging enable  
R4(config-archive-log-cfg)#end

# V-215810

The Cisco router must be configured to automatically audit account disabling actions.

Finding on device: **FAIL**

Rule Title: SRG-APP-000028-NDM-000210

Rule Severity: medium

Suggested Fix:

Configure the router to log account disabling using the following commands:  
  
R4(config)#archive  
R4(config-archive)#log config  
R4(config-archive-log-cfg)#logging enable  
R4(config-archive-log-cfg)#end

# V-215811

The Cisco router must be configured to automatically audit account removal actions.

Finding on device: **FAIL**

Rule Title: SRG-APP-000029-NDM-000211

Rule Severity: medium

Suggested Fix:

Configure the router to log account removal using the following commands:  
  
R4(config)#archive  
R4(config-archive)#log config  
R4(config-archive-log-cfg)#logging enable  
R4(config-archive-log-cfg)#end

# V-215819

The Cisco router must be configured to generate audit records containing the full-text recording of privileged commands.

Finding on device: **FAIL**

Rule Title: SRG-APP-000101-NDM-000231

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to log all configuration changes as shown in the example below.  
  
R4(config)#archive  
R4(config-archive)#log config  
R4(config-archive-log-cfg)#logging enable  
R4(config-archive-log-cfg)#end

# V-215821

The Cisco router must be configured to protect audit information from unauthorized deletion.

Finding on device: **FAIL**

Rule Title: SRG-APP-000120-NDM-000237

Rule Severity: medium

Suggested Fix:

If persistent logging is enabled, configure the router to only allow administrators with privilege level "15" access to the file system as shown in the example below.  
  
R4(config)#file privilege 15

# V-215822

The Cisco router must be configured to limit privileges to change the software resident within software libraries.

Finding on device: **FAIL**

Rule Title: SRG-APP-000133-NDM-000244

Rule Severity: medium

Suggested Fix:

Configure the router to only allow administrators with privilege level "15" access to the file system as shown in the example below.  
  
R4(config)#file privilege 15

# V-215834

The Cisco router must be configured to automatically audit account enabling actions.

Finding on device: **FAIL**

Rule Title: SRG-APP-000319-NDM-000283

Rule Severity: medium

Suggested Fix:

Configure the router to log account enabling using the following commands:  
  
R4(config)#archive  
R4(config-archive)#log config  
R4(config-archive-log-cfg)#logging enable  
R4(config-archive-log-cfg)#end

# V-215835

The Cisco router must be configured to audit the execution of privileged functions.

Finding on device: **FAIL**

Rule Title: SRG-APP-000343-NDM-000289

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to log all commands entered from the command line interface as well as log all configuration changes as shown in the following example:  
  
R1(config)#logging userinfo  
R1(config)#archive  
R1(config-archive)#log config  
R1(config-archive-log-cfg)#logging enable  
R1(config-archive-log-cfg)#end

# V-215839

The Cisco router must record time stamps for audit records that meet a granularity of one second for a minimum degree of precision.

Finding on device: **FAIL**

Rule Title: SRG-APP-000375-NDM-000300

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to record time stamps that meet a granularity of one second as shown in the example below.  
  
R2(config)#service timestamps log datetime localtime

# V-215847

The Cisco router must be configured to generate log records when administrator privileges are modified.

Finding on device: **FAIL**

Rule Title: SRG-APP-000495-NDM-000318

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to generate log records when account privileges are modified as shown in the example below.  
  
R4(config)#logging userinfo   
R4(config)#archive  
R4(config-archive)#log config  
R4(config-archive-log-cfg)#logging enable  
R4(config-archive-log-cfg)#end

# V-215848

The Cisco router must be configured to generate log records when administrator privileges are deleted.

Finding on device: **FAIL**

Rule Title: SRG-APP-000499-NDM-000319

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to generate log records when administrator privileges are deleted as shown in the example below.  
  
R4(config)#archive  
R4(config-archive)#log config  
R4(config-archive-log-cfg)#logging enable  
R4(config-archive-log-cfg)#end

# V-215849

The Cisco router must be configured to generate audit records when successful/unsuccessful logon attempts occur.

Finding on device: **FAIL**

Rule Title: SRG-APP-000503-NDM-000320

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to generate audit records when successful/unsuccessful logon attempts occur as shown in the example below.  
  
R5(config)#login on-failure log  
R5(config)#login on-success log

# V-215850

The Cisco router must be configured to generate log records for privileged activities.

Finding on device: **FAIL**

Rule Title: SRG-APP-000504-NDM-000321

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to generate log records for privileged activities as shown in the example below.  
  
R4(config)#archive  
R4(config-archive)#log config  
R4(config-archive-log-cfg)#logging enable  
R4(config-archive-log-cfg)#end

# V-215852

The Cisco router must be configured to generate log records when concurrent logons from different workstations occur.

Finding on device: **FAIL**

Rule Title: SRG-APP-000506-NDM-000323

Rule Severity: medium

Suggested Fix:

Configure the Cisco router to generate log records when concurrent logons from different workstations occur as shown in the example below.  
  
R5(config)#login on-success log

# V-216647

The Cisco router must be configured to have all non-essential capabilities disabled.

Finding on device: **PASS**

Rule Title: SRG-NET-000131-RTR-000035

Rule Severity: low