UNCLASSIFIED

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG)

6

Release: 12 Benchmark Date: 28 Oct 2016

This STIG contains the technical security controls for the operation of a WLAN access point (Internet Gateway Only Connection role) in the DoD environment.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Network devices must be password protected.
STIG ID: NET0230 **Rule ID:** SV-3012r4_rule **Vuln ID:** V-3012
Severity: CAT I **Class:** Unclass

Discussion:
Network access control mechanisms interoperate to prevent unauthorized access and to enforce the organization's security policy. Access to the network must be categorized as administrator, user, or guest so the appropriate authorization can be assigned to the user requesting access to the network or a network device. Authorization requires an individual account identifier that has been approved, assigned, and configured on an authentication server. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multi-factor authentication, some combination thereof. Lack of authentication enables anyone to gain access to the network or possibly a network device providing opportunity for intruders to compromise resources within the network infrastructure.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the network devices configuration to determine if administrative access to the device requires some form of authentication--at a minimum a password is required.

If passwords aren't used to administrative access to the device, this is a finding.

Fix Text:
Configure the network devices so it will require a password to gain administrative access to the device.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Network devices must display the DoD-approved logon banner warning.
STIG ID: NET0340 **Rule ID:** SV-3013r4_rule **Vuln ID:** V-3013
Severity: CAT II **Class:** Unclass

Discussion:
All network devices must present a DoD-approved warning banner prior to a system administrator logging on. The banner should warn any unauthorized user not to proceed. It also should provide clear and unequivocal notice to both authorized and unauthorized personnel that access to the device is subject to monitoring to detect unauthorized usage. Failure to display the required logon warning banner prior to logon attempts will limit DoD's ability to prosecute unauthorized access and also presents the potential to give rise to criminal and civil liability for systems administrators and information systems managers. In addition, DISA's ability to monitor the device's usage is limited unless a proper warning banner is displayed.

DoD CIO has issued new, mandatory policy standardizing the wording of "notice and consent" banners and matching user agreements for all Secret and below DoD information systems, including stand-alone systems by releasing DoD CIO Memo, "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement", dated 9 May 2008. The banner is mandatory and deviations are not permitted except as authorized in writing by the Deputy Assistant Secretary of Defense for Information and Identity Assurance. Implementation of this banner verbiage is further directed to all DoD components for all DoD assets via USCYBERCOM CTO 08-008A.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the device configuration or request that the administrator logon to the device and observe the terminal. Verify either Option A or Option B (for systems with character limitations) of the Standard Mandatory DoD Notice and Consent Banner is displayed at logon. The required banner verbiage follows and must be displayed verbatim:

Option A

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.

Option B

If the system is incapable of displaying the required banner verbiage due to its size, a smaller banner must be used. The mandatory verbiage follows: "I've read & consent to terms in IS user agreem't."

If the device configuration does not have a logon banner as stated above, this is a finding.

Fix Text:
Configure all management interfaces to the network device to display the DoD-mandated warning banner verbiage at logon regardless of the means of connection or communication. The required banner verbiage that must be displayed verbatim is as follows:

Option A

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.

Option B

If the system is incapable of displaying the required banner verbiage due to its size, a smaller banner must be used. The mandatory verbiage follows: "I've read & consent to terms in IS user agreem't."

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network devices must timeout management connections for administrative access after 10 minutes or less of inactivity.
STIG ID: NET1639 **Rule ID:** SV-3014r4_rule **Vuln ID:** V-3014
Severity: CAT II **Class:** Unclass

Discussion:
Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled between the managed network device and a PC or terminal server when the later has been left unattended. In addition quickly terminating an idle session will also free up resources committed by the managed network device as well as reduce the risk of a management session from being hijacked. Setting the timeout of the session to 10 minutes or less increases the level of protection afforded critical network components.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the management connection for administrative access and verify the network device is configured to time-out the connection at 10 minutes or less of inactivity.

If the device does not terminate inactive management connections at 10 minutes or less, this is a finding.

Fix Text:
Configure the network devices to ensure the timeout for unattended administrative access connections is no longer than 10 minutes.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Group accounts must not be configured for use on the network device.
STIG ID: NET0460 **Rule ID:** SV-3056r7_rule **Vuln ID:** V-3056
Severity: CAT I **Class:** Unclass

Discussion:
Group accounts configured for use on a network device do not allow for accountability or repudiation of individuals using the shared account. If group accounts are not changed when someone leaves the group, that person could possibly gain control of the network device. Having group accounts does not allow for proper auditing of who is accessing or changing the network.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the network device configuration and validate there are no group accounts configured for access.

If a group account is configured on the device, this is a finding.

Fix Text:
Configure individual user accounts for each authorized person then remove any group accounts.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Authorized accounts must be assigned the least privilege level necessary to perform assigned duties.
STIG ID: NET0465 **Rule ID:** SV-3057r5_rule **Vuln ID:** V-3057
Severity: CAT II **Class:** Unclass

Discussion:
By not restricting authorized accounts to their proper privilege level, access to restricted functions may be allowed before authorized personnel are trained or experienced enough to use those functions. Network disruptions or outages may occur due to mistakes made by inexperienced persons using accounts with greater privileges than necessary.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the accounts authorized for access to the network device. Determine if the accounts are assigned the lowest privilege level necessary to perform assigned duties. User accounts must be set to a specific privilege level which can be mapped to specific commands or a group of commands. Authorized accounts should have the greatest privilege level unless deemed necessary for assigned duties.

If it is determined that authorized accounts are assigned to greater privileges than necessary, this is a finding.

Fix Text:
Configure authorized accounts with the least privilege rule. Each user will have access to only the privileges they require to perform their assigned duties.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Unauthorized accounts must not be configured for access to the network device.
STIG ID: NET0470 **Rule ID:** SV-3058r5_rule **Vuln ID:** V-3058
Severity: CAT II **Class:** Unclass

Discussion:
A malicious user attempting to gain access to the network device may compromise an account that may be unauthorized for use. The unauthorized account may be a temporary or inactive account that is no longer needed to access the device. Denial of Service, interception of sensitive information, or other destructive actions could potentially take place if an unauthorized account is configured to access the network device.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the organization's responsibilities list and reconcile the list of authorized accounts with those accounts defined for access to the network device.

If an unauthorized account is configured for access to the device, this is a finding.

Fix Text:
Remove any account configured for access to the network device that is not defined in the organization's responsibilities list.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Management connections to a network device must be established using secure protocols with FIPS 140-2 validated cryptographic modules.
STIG ID: NET1638 **Rule ID:** SV-3069r5_rule **Vuln ID:** V-3069
Severity: CAT II **Class:** Unclass

Discussion:
Administration and management connections performed across a network are inherently dangerous because anyone with a packet sniffer and access to the right LAN segment can acquire the network device account and password information. With this intercepted information they could gain access to the router and cause denial of service attacks, intercept sensitive information, or perform other destructive actions.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the network device configuration to verify only secure protocols using FIPS 140-2 validated cryptographic modules are

used for any administrative access. Some of the secure protocols used for administrative and management access are listed below. This list is not all inclusive and represents a sample selection of secure protocols.

-SSHv2
-SCP
-HTTPS using TLS

If management connections are established using protocols without FIPS 140-2 validated cryptographic modules, this is a finding.

Fix Text:
Configure the network device to use secure protocols with FIPS 140-2 validated cryptographic modules.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Network devices must log all attempts to establish a management connection for administrative access.
STIG ID: NET1640 **Rule ID:** SV-3070r4_rule **Vuln ID:** V-3070
Severity: CAT III **Class:** Unclass

Discussion:
Audit logs are necessary to provide a trail of evidence in case the network is compromised. Without an audit trail that provides a when, where, who and how set of information, repeat offenders could continue attacks against the network indefinitely. With this information, the network administrator can devise ways to block the attack and possibly identify and prosecute the attacker.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the configuration to verify all attempts to access the device via management connection are logged.

If management connection attempts are not logged, this is a finding.

Fix Text:
Configure the device to log all access attempts to the device to establish a management connection for administrative access.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Network devices must not have any default manufacturer passwords.
STIG ID: NET0240 **Rule ID:** SV-3143r4_rule **Vuln ID:** V-3143
Severity: CAT I **Class:** Unclass

Discussion:
Network devices not protected with strong password schemes provide the opportunity for anyone to crack the password thus gaining access to the device and causing network outage or denial of service. Many default vendor passwords are well-known; hence, not removing them prior to deploying the network devices into production provides an opportunity for a malicious user to gain unauthorized access to the device.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the network devices configuration to determine if the vendor default password is active.

If any vendor default passwords are used on the device, this is a finding.

Fix Text:
Remove any vendor default passwords from the network devices configuration.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Network devices must be running a current and supported operating system with all IAVMs addressed.
STIG ID: NET0700 **Rule ID:** SV-3160r4_rule **Vuln ID:** V-3160
Severity: CAT II **Class:** Unclass

Discussion:
Network devices not running the latest tested and approved versions of software are vulnerable to network attacks. Running the most current, approved version of system and device software helps the site maintain a stable base of security fixes and patches, as well as enhancements to IP security. Viruses, denial of service attacks, system weaknesses, back doors and other potentially harmful situations could render a system vulnerable, allowing unauthorized access to DoD assets.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Have the administrator display the OS version in operation. The OS must be current with related IAVMs addressed.

If the device is using an OS that does not meet all IAVMs or currently not supported by the vendor, this is a finding.

Fix Text:
Update operating system to a supported version that addresses all related IAVMs.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network device must require authentication prior to establishing a management connection for administrative access.
STIG ID: NET1636 **Rule ID:** SV-3175r5_rule **Vuln ID:** V-3175
Severity: CAT I **Class:** Unclass

Discussion:
Network devices with no password for administrative access via a management connection provide the opportunity for anyone with network access to the device to make configuration changes enabling them to disrupt network operations resulting in a network outage.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the network device configuration to verify all management connections for administrative access require authentication.

If authentication isn't configured for management access, this is a finding.

Fix Text:
Configure authentication for all management connections.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network device must use SNMP Version 3 Security Model with FIPS 140-2 validated cryptography for any SNMP agent configured on the device.
STIG ID: NET1660 **Rule ID:** SV-3196r4_rule **Vuln ID:** V-3196
Severity: CAT I **Class:** Unclass

Discussion:
SNMP Versions 1 and 2 are not considered secure. Without the strong authentication and privacy that is provided by the SNMP Version 3 User-based Security Model (USM), an unauthorized user can gain access to network management information used to launch an attack against the network.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the device configuration to verify it is configured to use SNMPv3 with both SHA authentication and privacy using AES encryption.

Downgrades:
If the site is using Version 1 or Version 2 with all of the appropriate patches and has developed a migration plan to implement the Version 3 Security Model, this finding can be downgraded to a Category II.

If the targeted asset is running SNMPv3 and does not support SHA or AES, but the device is configured to use MD5 authentication and DES or 3DES encryption, then the finding can be downgraded to a Category III.

If the site is using Version 1 or Version 2 and has installed all of the appropriate patches or upgrades to mitigate any known security vulnerabilities, this finding can be downgraded to a Category II. In addition, if the device does not support SNMPv3, this finding can be downgraded to a Category III provided all of the appropriate patches to mitigate any known security vulnerabilities have been applied and has developed a migration plan that includes the device upgrade to support Version 3 and the implementation of the Version 3 Security Model.

If the device is configured to use to anything other than SNMPv3 with at least SHA-1 and AES, this is a finding. Downgrades can be determined based on the criteria above.

Fix Text:
If SNMP is enabled, configure the network device to use SNMP Version 3 Security Model with FIPS 140-2 validated cryptography (i.e., SHA authentication and AES encryption).

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network device must not use the default or well-known SNMP community strings public and private.
STIG ID: NET1665 **Rule ID:** SV-3210r4_rule **Vuln ID:** V-3210
Severity: CAT I **Class:** Unclass

Discussion:
Network devices may be distributed by the vendor pre-configured with an SNMP agent using the well-known SNMP community strings public for read only and private for read and write authorization. An attacker can obtain information about a network device using the read community string "public". In addition, an attacker can change a system configuration using the write community string "private".

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the network devices configuration and verify if either of the SNMP community strings "public" or "private" is being used.

If default or well-known community strings are used for SNMP, this is a finding.

Fix Text:
Configure unique SNMP community strings replacing the default community strings.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: In the event the authentication server is unavailable, the network device must have a single local account of last resort defined.
STIG ID: NET0440 **Rule ID:** SV-3966r6_rule **Vuln ID:** V-3966
Severity: CAT II **Class:** Unclass

Discussion:
Authentication for administrative access to the device is required at all times. A single account of last resort can be created on the device's local database for use in an emergency such as when the authentication server is down or connectivity between the device and the authentication server is not operable. The console or local account of last resort logon credentials must be stored in a sealed envelope and kept in a safe.

Documentable: No

Check Content:
Review the network device configuration to determine if an authentication server is defined for gaining administrative access. If so, there must be only one account of last resort configured locally for an emergency.

Verify the username and password for the local account of last resort is contained within a sealed envelope kept in a safe.

If an authentication server is used and more than one local account exists, this is a finding.

Fix Text:
Configure the device to only allow one local account of last resort for emergency access and store the credentials in a secure manner.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network devices must time out access to the console port at 10 minutes or less of inactivity.
STIG ID: NET1624 **Rule ID:** SV-3967r4_rule **Vuln ID:** V-3967
Severity: CAT II **Class:** Unclass

Discussion:
Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition quickly terminating an idle session will also free up resources committed by the managed network device. Setting the timeout of the session to 10 minutes or less increases the level of protection afforded critical network components.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the configuration and verify a session using the console port will time out after 10 minutes or less of inactivity.

If console access is not configured to timeout at 10 minutes or less, this is a finding.

Fix Text:
Configure the timeout for idle console connection to 10 minutes or less.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Network devices must only allow SNMP read-only access.
STIG ID: NET0894 **Rule ID:** SV-3969r5_rule **Vuln ID:** V-3969
Severity: CAT II **Class:** Unclass

Discussion:
Enabling write access to the device via SNMP provides a mechanism that can be exploited by an attacker to set configuration variables that can disrupt network operations.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the network device configuration and verify SNMP community strings are read-only when using SNMPv1, v2c, or basic v3 (no authentication or privacy). Write access may be used if authentication is configured when using SNMPv3.

If write-access is used for SNMP versions 1, 2c, or 3-noAuthNoPriv mode and there is no documented approval by the ISSO, this is a finding.

Fix Text:
Configure the network device to allow for read-only SNMP access when using SNMPv1, v2c, or basic v3 (no authentication or privacy). Write access may be used if authentication is configured when using SNMPv3.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network device must require authentication for console access.
STIG ID: NET1623 **Rule ID:** SV-4582r5_rule **Vuln ID:** V-4582
Severity: CAT I **Class:** Unclass

Discussion:
Network devices with no password for administrative access via the console provide the opportunity for anyone with physical access to the device to make configuration changes enabling them to disrupt network operations resulting in a network outage.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the network device's configuration and verify authentication is required for console access.

If authentication is not configured for console access, this is a finding.

Fix Text:
Configure authentication for console access on the network device.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network devices must only allow management connections for administrative access from hosts residing in the management network.

STIG ID: NET1637 **Rule ID:** SV-5611r5_rule **Vuln ID:** V-5611
Severity: CAT II **Class:** Unclass

Discussion:
Remote administration is inherently dangerous because anyone with a sniffer and access to the right LAN segment could acquire the device account and password information. With this intercepted information they could gain access to the infrastructure and cause denial of service attacks, intercept sensitive information, or perform other destructive actions.

Documentable: No

Check Content:
Review the configuration and verify management access to the device is allowed only from hosts within the management network.

If management access can be gained from outside of the authorized management network, this is a finding.

Fix Text:
Configure an ACL or filter to restrict management access to the device from only the management network.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network device must be configured for a maximum number of unsuccessful SSH logon attempts set at 3 before resetting the interface.
STIG ID: NET1646 **Rule ID:** SV-5613r4_rule **Vuln ID:** V-5613
Severity: CAT II **Class:** Unclass

Discussion:
An attacker may attempt to connect to the device using SSH by guessing the authentication method and authentication key or shared secret. Setting the authentication retry to 3 or less strengthens against a Brute Force attack.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the configuration and verify the number of unsuccessful SSH logon attempts is set at 3.

If the device is not configured to reset unsuccessful SSH logon attempts at 3, this is a finding.

Fix Text:
Configure the network device to require a maximum number of unsuccessful SSH logon attempts at 3.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The auxiliary port must be disabled unless it is connected to a secured modem providing encryption and authentication.
STIG ID: NET1629 **Rule ID:** SV-7365r4_rule **Vuln ID:** V-7011
Severity: CAT III **Class:** Unclass

Discussion:
The use of POTS lines to modems connecting to network devices provides clear text of authentication traffic over commercial circuits that could be captured and used to compromise the network. Additional war dial attacks on the device could degrade the device and the production network.

Secured modem devices must be able to authenticate users and must negotiate a key exchange before full encryption takes

place. The modem will provide full encryption capability (Triple DES) or stronger. The technician who manages these devices will be authenticated using a key fob and granted access to the appropriate maintenance port, thus the technician will gain access to the managed device (router, switch, etc.). The token provides a method of strong (two-factor) user authentication. The token works in conjunction with a server to generate one-time user passwords that will change values at second intervals. The user must know a personal identification number (PIN) and possess the token to be allowed access to the device.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the configuration and verify the auxiliary port is disabled unless a secured modem providing encryption and authentication is connected.

If the auxiliary port is enabled without the use of a secured modem, this is a finding.

Fix Text:
Disable the auxiliary port. If used for out-of-band administrative access, the port must be connected to a secured modem providing encryption and authentication.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Network devices must authenticate all NTP messages received from NTP servers and peers.
STIG ID: NET0813 **Rule ID:** SV-15327r5_rule **Vuln ID:** V-14671
Severity: CAT II **Class:** Unclass

Discussion:
Since NTP is used to ensure accurate log file time stamp information, NTP could pose a security risk if a malicious user were able to falsify NTP information. To launch an attack on the NTP infrastructure, a hacker could inject time that would be accepted by NTP clients by spoofing the IP address of a valid NTP server. To mitigate this risk, the time messages must be authenticated by the client before accepting them as a time source.

Two NTP-enabled devices can communicate in either client-server mode or peer-to-peer mode (aka "symmetric mode"). The peering mode is configured manually on the device and indicated in the outgoing NTP packets. The fundamental difference is the synchronization behavior: an NTP server can synchronize to a peer with better stratum, whereas it will never synchronize to its client regardless of the client's stratum. From a protocol perspective, NTP clients are no different from the NTP servers. The NTP client can synchronize to multiple NTP servers, select the best server and synchronize with it, or synchronize to the averaged value returned by the servers.

A hierarchical model can be used to improve scalability. With this implementation, an NTP client can also become an NTP server providing time to downstream clients at a higher stratum level and of decreasing accuracy than that of its upstream server. To increase availability, NTP peering can be used between NTP servers. In the event the device loses connectivity to its upstream NTP server, it will be able to choose time from one of its peers.

The NTP authentication model is opposite of the typical client-server authentication model. NTP authentication enables an NTP client or peer to authenticate time received from their servers and peers. It is not used to authenticate NTP clients because NTP servers do not care about the authenticity of their clients, as they never accept any time from them.

Documentable: No

Check Content:
Review the network element configuration and verify that it is authenticating NTP messages received from the NTP server or peer using either PKI or a FIPS-approved message authentication code algorithm. FIPS-approved algorithms for authentication are the cipher-based message authentication code (CMAC) and the keyed-hash message authentication code (HMAC). AES and 3DES are NIST-approved CMAC algorithms. The following are NIST-approved HMAC algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256.

If the network element is not configured to authenticate received NTP messages using PKI or a FIPS-approved message authentication code algorithm, this is a finding.

Fix Text:
Configure the device to authenticate all received NTP messages using either PKI (supported in NTP v4) or a FIPS-approved message authentication code algorithm.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network device must not allow SSH Version 1 to be used for administrative access.
STIG ID: NET1647 **Rule ID:** SV-15459r4_rule **Vuln ID:** V-14717
Severity: CAT II **Class:** Unclass

Discussion:
SSH Version 1 is a protocol that has never been defined in a standard. Since SSH-1 has inherent design flaws which make it vulnerable to attacks, e.g., man-in-the-middle attacks, it is now generally considered obsolete and should be avoided by explicitly disabling fallback to SSH-1.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the configuration and verify SSH Version 1 is not being used for administrative access.

If the device is using an SSHv1 session, this is a finding.

Fix Text:
Configure the network device to use SSH version 2.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: WLAN SSIDs must be changed from the manufacturerâ€™s default to a pseudo random word that does not identify the unit, base, organization, etc.
STIG ID: WIR0105 **Rule ID:** SV-15614r1_rule **Vuln ID:** V-14846
Severity: CAT III **Class:** Unclass

Discussion:
An SSID identifying the unit, site or purpose of the WLAN or is set to the manufacturer default may cause an OPSEC vulnerability.

Documentable: No

Responsibility:
System Administrator

Check Content:
Review device configuration.
1. Obtain the SSID using a wireless scanner or the AP or WLAN controller management software.
2. Verify the name is not meaningful (e.g., site name, product name, room number, etc.) or set to the manufacturer's default value.

Mark as a finding if the SSID does not meet the requirement listed above.

Fix Text:
Change the SSID to a pseudo random word that does not identify the unit, base, or organization.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The WLAN inactive session timeout must be set for 30 minutes or less.

STIG ID: WIR0110 **Rule ID:** SV-15656r1_rule **Vuln ID:** V-14888
Severity: CAT II **Class:** Unclass

Discussion:
A WLAN session that never terminates due to inactivity may allow an opening for an adversary to highjack the session to obtain access to the network.

Documentable: No

Responsibility:
System Administrator

Check Content:
1. Review the relevant configuration screen of the WLAN controller or access point.
2. Verify the session timeout setting is set for 30 minutes or less.
4. Mark as a finding if any of the following are found.
- Session timeout is not set to 30 minutes or less for the entire WLAN.
- The WLAN does not have the capability to enable the session time-out feature.

Fix Text:
Set the WLAN inactive session timeout to 30 minutes or less.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: WLAN signals must not be intercepted outside areas authorized for WLAN access.
STIG ID: WIR0120 **Rule ID:** SV-15657r1_rule **Vuln ID:** V-14889
Severity: CAT III **Class:** Unclass

Discussion:
Vulnerability Discussion: Most commercially-available WLAN equipment is pre-configured for signal power appropriate to most applications of the WLAN equipment. In some cases, this may permit the signals to be received outside the physical areas for which they are intended. This may occur when the intended area is relatively small, such as a conference room, or when the access point is placed near or window or wall, thereby allowing signals to be received in neighboring areas. In such cases, an adversary may be able to compromise the site's OPSEC posture by measuring the presence of the signal and the quantity of data transmitted to obtain information about when personnel are active and what they are doing. Furthermore, if the signal is not appropriately protected through defense-in-depth mechanisms, the adversary could possibly use the connection to access DoD networks and sensitive information.

Documentable: No

Responsibility:
System Administrator

Check Content:
Review documentation and inspect AP locations.

1. Review documentation showing signal strength analysis from site survey activities, if available.
2. Use testing equipment or WLAN clients to determine if the signal strength is, in the reviewer's judgment, excessively outside the required area (e.g., strong signal in the parking area, public areas, or uncontrolled spaces).
3. Lower end APs will not have this setting available—in this case, the site should locate the APs away from exterior walls to achieve compliance with this requirement.
4. Mark as a finding if any of the following is found.
o Visual inspection of equipment shows obvious improper placement of APs where it will emanate into uncontrolled spaces (e.g., next to external walls, windows, or doors; uncontrolled areas; or public areas).
o Building walk-through testing shows signals of sufficient quality and strength to allow wireless access to exist in areas not authorized for WLAN access.

Fix Text:
Move APs to areas in which signals do not emanate in a manner making them usable outside the areas authorized for WLAN access. Alternatively, replace omni-directional antennae with directional antennae if this will solve the problem. If these solutions are not effective, then adjust the transmission power settings on the AP to reduce the usability of signals in unauthorized areas. If the WLAN equipment does not allow the transmission power to be adjusted, and the APs are placed in a location where the IAO determines there is significant risk that an adversary could be present in location where signals may be

intercepted, then the site should procure WLAN equipment that permits power adjustment.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Network devices must use two or more authentication servers for the purpose of granting administrative access.
STIG ID: NET0433 **Rule ID:** SV-16259r4_rule **Vuln ID:** V-15432
Severity: CAT II **Class:** Unclass

Discussion:
The use of Authentication, Authorization, and Accounting (AAA) affords the best methods for controlling user access, authorization levels, and activity logging. By enabling AAA on the routers in conjunction with an authentication server such as TACACS+ or RADIUS, the administrators can easily add or remove user accounts, add or remove command authorizations, and maintain a log of user activity.

The use of an authentication server provides the capability to assign router administrators to tiered groups that contain their privilege level that is used for authorization of specific commands. For example, user mode would be authorized for all authenticated administrators while configuration or edit mode should only be granted to those administrators that are permitted to implement router configuration changes.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Verify an authentication server is required to access the device and that there are two or more authentication servers defined.

If the device is not configured for two separate authentication servers, this is a finding.

Fix Text:
Configure the device to use two separate authentication servers.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The emergency administration account must be set to an appropriate authorization level to perform necessary administrative functions when the authentication server is not online.
STIG ID: NET0441 **Rule ID:** SV-16261r5_rule **Vuln ID:** V-15434
Severity: CAT I **Class:** Unclass

Discussion:
The emergency administration account is to be configured as a local account on the network devices. It is to be used only when the authentication server is offline or not reachable via the network. The emergency account must be set to an appropriate authorization level to perform necessary administrative functions during this time.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the emergency administration account configured on the network devices and verify that it has been assigned to a privilege level that will enable the administrator to perform necessary administrative functions when the authentication server is not online.

If the emergency administration account is configured for more access than needed to troubleshoot issues, this is a finding.

Fix Text:
Assign a privilege level to the emergency administration account to allow the administrator to perform necessary administrative

functions when the authentication server is not online.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network devices OOBM interface must be configured with an OOBM network address.
STIG ID: NET0991 **Rule ID:** SV-19075r4_rule **Vuln ID:** V-17821
Severity: CAT II **Class:** Unclass

Discussion:
The OOBM access switch will connect to the management interface of the managed network device. The management interface of the managed network device will be directly connected to the OOBM network. An OOBM interface does not forward transit traffic; thereby, providing complete separation of production and management traffic. Since all management traffic is immediately forwarded into the management network, it is not exposed to possible tampering. The separation also ensures that congestion or failures in the managed network do not affect the management of the device. If the OOBM interface does not have an IP address from the managed network address space, it will not have reachability from the NOC using scalable and normal control plane and forwarding mechanisms.

Documentable: No

Responsibility:
System Administrator

Check Content:
Review the device configuration to determine if the OOB management interface is assigned an appropriate IP address from the authorized OOB management network.

If an IP address assigned to the interface is not from an authorized OOB management network, this is a finding.

Fix Text:
Configure the OOB management interface with an IP address from the address space belonging to the OOBM network.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The network devices management interface must be configured with both an ingress and egress ACL.
STIG ID: NET0992 **Rule ID:** SV-19076r4_rule **Vuln ID:** V-17822
Severity: CAT II **Class:** Unclass

Discussion:
The OOBM access switch will connect to the management interface of the managed network device. The management interface can be a true OOBM interface or a standard interface functioning as the management interface. In either case, the management interface of the managed network device will be directly connected to the OOBM network.

An OOBM interface does not forward transit traffic; thereby, providing complete separation of production and management traffic. Since all management traffic is immediately forwarded into the management network, it is not exposed to possible tampering. The separation also ensures that congestion or failures in the managed network do not affect the management of the device. If the device does not have an OOBM port, the interface functioning as the management interface must be configured so that management traffic does not leak into the managed network and that production traffic does not leak into the management network.

Documentable: No

Responsibility:
System Administrator

Check Content:
Step 1: Verify the managed interface has an inbound and outbound ACL or filter.

Step 2: Verify the ingress ACL blocks all transit traffic--that is, any traffic not destined to the router itself. In addition, traffic

accessing the managed elements should be originated at the NOC.

Step 3: Verify the egress ACL blocks any traffic not originated by the managed element.

If management interface does not have an ingress and egress filter configured and applied, this is a finding.

Fix Text:
If the management interface is a routed interface, it must be configured with both an ingress and egress ACL. The ingress ACL should block any transit traffic, while the egress ACL should block any traffic that was not originated by the managed network device.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: Network devices must use at least two NTP servers to synchronize time.
STIG ID: NET0812 **Rule ID:** SV-28651r4_rule **Vuln ID:** V-23747
Severity: CAT III **Class:** Unclass

Discussion:
Without synchronized time, accurately correlating information between devices becomes difficult, if not impossible. If logs cannot be successfully compared between each of the routers, switches, and firewalls, it will be very difficult to determine the exact events that resulted in a network breach incident. NTP provides an efficient and scalable method for network devices to synchronize to an accurate time source.

Documentable: No

Responsibility:
System Administrator

Check Content:
Review the configuration and verify two NTP servers have been defined.

If the device is not configured to use two separate NTP servers, this is a finding.

Fix Text:
Configure the device to use two separate NTP servers.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: WLAN access point must be configured for Wi-Fi Alliance WPA2 security.
STIG ID: WIR0121 **Rule ID:** SV-31426r1_rule **Vuln ID:** V-25315
Severity: CAT II **Class:** Unclass

Discussion:
The Wi-Fi Alliance’s WPA2 certification provides assurance that the device has adequate security functionality and can implement the IEEE 802.11i standard for robust security networks. The previous version of the Wi-Fi Alliance certification, WPA, did not require AES encryption, which must be supported for DoD WLAN implementations. Devices without any WPA certification likely do not support required security functionality and could be vulnerable to a wide range of attacks.

Documentable: No

Responsibility:
System Administrator

Check Content:
Verify the access point is configured for either WPA2 (Enterprise) or WPA2 (Personal) authentication. The procedure for performing this review will vary depending on the AP model. Have the SA show the configuration setting.

Fix Text:
Configure the access point for WPA2 authentication, confidentiality, and integrity services. In the case of WPA2 (Personal), this action will require the selection of a strong passcode or passphrase. In the case of WPA2 (Enterprise), this action will require the organization to deploy RADIUS or equivalent authentication services on a separate server. In cases in which the access point does not support WPA2, the organization will need to procure new equipment.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: The password configured on the WLAN Access Point for key generation and client access must be set to a 14 character or longer complex password as required by USCYBERCOM CTO 07-15Rev1.
STIG ID: WIR0122 **Rule ID:** SV-31427r2_rule **Vuln ID:** V-25316
Severity: CAT II **Class:** Unclass

Discussion:
If the organization does not use a strong passcode for client access, then it is significantly more likely that an adversary will be able to obtain it. Once this occurs, the adversary may be able to obtain full network access, obtain DoD sensitive information, and attack other DoD information systems.

Documentable: No

Responsibility:
System Administrator

Check Content:
This check only applies to access points that do not use an AAA (RADIUS) server for authentication services. In most cases, this means the access point is configured for WPA2 (Personal), which relies on password authentication, and not WPA2 (Enterprise) which uses an AAA server to authenticate each user based on that user’s authentication credentials.
Verify the client authentication password has been set on the access point with the following settings:

-14 characters or longer.
-The authentication password selected must be comprised of at least two of each of the following: upper case letter, lower case letter, number, and special character.

The procedure for verifying these settings varies between AP models. Have the SA show the settings in the AP management console.

Fix Text:
The key generation password configured on the WLAN Access Point must be set to a 14-character or longer complex password on access points that do not use AAA servers for authentication.

WLAN Access Point (Internet Gateway Only Connection) Security Technical Implementation Guide (STIG) :: Release: 12
Benchmark Date: 28 Oct 2016
Rule Title: A service or feature that calls home to the vendor must be disabled.
STIG ID: NET0405 **Rule ID:** SV-36774r4_rule **Vuln ID:** V-28784
Severity: CAT II **Class:** Unclass

Discussion:
Call home services or features will routinely send data such as configuration and diagnostic information to the vendor for routine or emergency analysis and troubleshooting. The risk that transmission of sensitive data sent to unauthorized persons could result in data loss or downtime due to an attack.

Documentable: No

Responsibility:
Information Assurance Officer

Check Content:
Review the device configuration to determine if the call home service or feature is disabled on the device. If the call home service is enabled on the device, this is a finding.

Fix Text:
Configure the network device to disable the call home service or feature.