CIS Tanium 7.x Operating System on TanOS STIG Benchmark

v1.0.0 - 08-26-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Tanium 7.x Operating System on TanOS Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Tanium 7.x Operating System on TanOS and are looking to comply with the STIG guidance

Recommendation Definitions

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Tanium 7.x Operating System on TanOS

Recommendations

1 STIG RULES

Tanium 7.x Operating System on TanOS

Tanium 7.x Operating System on TanOS Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 TANS-OS-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.

```
GROUP ID: V-254839
RULE ID: SV-254839r1067738
```

Rationale:

By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu," and then press "Enter".
4. Press "L" for "Local Tanium User Management," and then press "Enter".
5. Press "B" for "Security Policy Local Authentication Service," and then press "Enter".

If the value of "Password Maximum Failure:" is greater than "3", this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu," and then press "Enter".
4. Press "L" for "Local Tanium User Management," and then press "Enter".
5. Press "B" for "Security Policy Local Authentication Service," and then press "Enter".
6. Type "yes," and then press "Enter".
7. Input the following settings pressing "Enter" after every value:
8. a) Minimum Password Lifetime: Configure an appropriate value
9. b) Maximum Password Lifetime: Configure an appropriate value
10. c) Minimum Password Length: Configure an appropriate value
11. d) Minimum Password History: Configure an appropriate value
12. e) Password Lockout: Configure an appropriate value
13. f) Password Maximum Failure: 3
14. Type "yes" to accept the new password policy.

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

1.2 TANS-OS-000075 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system.

```
GROUP ID: V-254840
RULE ID: SV-254840r958390
```

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060. Use the following verbiage for operating system that can accommodate banners of 1300 characters: "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."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read & consent to terms in IS user agreem't."
```

Audit:

1. Access the Tanium Server interactively.
2. Verify DOD use notification displayed prior to login.

"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."
If a DOD-approved use notification banner does not display prior to logon, this is a finding.

Remediation:

1. Create a .txt file composed of the DOD-authorized warning banner verbiage.

"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."

2. Name the file "banner_ssh.txt".
3. Use SFTP to upload the HTML banner file to the /incoming folder.
4. Access the Tanium Server interactively.
5. Log on to the TanOS server with the tanadmin role, or any additional user with administrative privileges.
6. Enter A: Appliance Configuration Menu >> A: Security >> 3: Configure SSH Banner and follow the prompts.
7. Log off and back on to the Tanium Server to confirm application.

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

1.3 TANS-OS-000095 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must limit the number of concurrent sessions to an organization-defined number for all accounts and/or account types.

```
GROUP ID: V-254841
RULE ID: SV-254841r958398
```

Rationale:

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press "P" for "Security Policy," and then press "Enter".
6. Press "M" for "Maximum Concurrent Logins," and then press "Enter".
7. Work with the Tanium Administrator to confirm the number of maximum concurrent users.

If the value of "Maximum Concurrent Logins:" is greater than the approved value, this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press P for "Security Policy," and then press "Enter".
6. Press "M" for "Maximum Concurrent Logins," and then press "Enter".
7. Work with the Tanium Administrator to set the number of maximum concurrent users.

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.4 TANS-OS-000165 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium operating system (TanOS) must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.

```
GROUP ID: V-254842
RULE ID: SV-254842r958424
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press 4 for "Syslog Configuration," and then press "Enter".
4. Press "1" for "Check current status," and then press Enter.

If the syslog status page states, "No existing TanOS syslog forwarding configuration found", this is a finding.
If the syslog status page states, "Syslog forwarding configuration" and the SIEM administrator verifies SIEM is receiving the events correctly and generating notifications for audit processing failure events, this is not a finding.

Remediation:

1. Access the TanOS interactively.
2. Press A for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press 5 for "Configure syslog forwarding," and then press "Enter".
5. Enter the destination host (IP address or hostname) provided by the SIEM administrator, and then press "Enter".
6. Enter the destination port number and press "Enter".
7. If TLS is required for this syslog destination, enter "Yes", otherwise enter "No", and then press "Enter".
8. Enter the destination protocol, "udp" or "tcp", and then press "Enter".
9. Work with the SIEM administrator to validate events are being received, and to configure notifications for audit processing failure events.

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

1.5 TANS-OS-000270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must enforce 24 hours/one day as the maximum password lifetime.

```
GROUP ID: V-254843
RULE ID: SV-254843r1015851
```

Rationale:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, then the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu".
4. Press "L" for "Local Tanium User Management".
5. Press "B" for "Security Policy Local Authentication Service".

If the "Password Minimum Age (days)" is not set to "1", this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu".
4. Press "L" for "Local Tanium User Management".
5. Press "B" for "Security Policy Local Authentication Service".
6. Type "Yes".
7. Set the value for "Define the minimum password in days [0 - 20]" to "1".
8. Press "Enter" to accept the current values for the rest of the options.
9. Type "Yes" to apply the new security policy.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000198 The information system enforces minimum password lifetime restrictions.

- NIST SP 800-53::IA-5 (1) (d)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (d)

1.6 TANS-OS-000275 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must enforce a 60-day maximum password lifetime restriction.

```
GROUP ID: V-254844
RULE ID: SV-254844r1038967
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically.

One method of minimizing this risk is to use complex passwords and periodically change them. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu".
4. Press "L" for "Local Tanium User Management".
5. Press "B" for "Security Policy Local Authentication Service".

If the "Password Maximum Age (days)" is not set to "60", this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu".
4. Press "L" for "Local Tanium User Management".
5. Press "B" for "Security Policy Local Authentication Service".
6. Type "Yes".
7. Press "Enter" to accept the current value for "Define the minimum password in days [0 - 20]".
8. Set the value of "Define the maximum password lifetime in days [0-300]" to "60".
9. Press "Enter" to accept the current values for the rest of the options.
10. Type "Yes" to apply the new security policy.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000199 The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53::IA-5 (1) (d)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (d)

1.7 TANS-OS-000285 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must enforce a minimum 15-character password length.

```
GROUP ID: V-254846
RULE ID: SV-254846r1067740
```

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu".
4. Press "L" for "Local Tanium User Management".
5. Press "B" for "Security Policy Local Authentication Service".

If "Password Minimum Length" is not set to 15, this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu".
4. Press "L" for "Local Tanium User Management".
5. Press "B" for "Security Policy Local Authentication Service".
6. Type "Yes".
7. Press "Enter" to accept the current value for "Minimum password lifetime in days [0 - 20]:".
8. Press "Enter" to accept the current value for "Maximum password lifetime in days [MinAge - 360]:".
9. Set the value for "Minimum password length in characters [0 - 30]:" to "15".
10. Press "Enter" to accept the current values for the rest of the options.
11. Type "Yes" to apply the new security policy.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000205 The information system enforces minimum password length.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (i)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.8 TANS-OS-000325 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Tanium Operating System (TanOS) must use multifactor authentication for network access to privileged accounts.

```
GROUP ID: V-254847
RULE ID: SV-254847r986546
```

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include: (i) Something a user knows (e.g., password/PIN); (ii) Something a user has (e.g., cryptographic identification device, token); or (iii) Something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).

The DOD CAC with DOD-approved PKI is an example of multifactor authentication.

Audit:

1. Sign in to the TanOS console as a user with the tanadmin role.
2. Enter "C" to go to the "User Administration" menu.
3. Enter "M" to go to the "Multi-Factor Global Settings" menu.
4. If the status shows "Multi-Factor: Optional", this is a finding.

Remediation:

1. Sign in to the TanOS console as a user with the tanadmin role.
2. Enter "C" to go to the "User Administration" menu.
3. Enter "M" to go to the "Multi-Factor Global Settings" menu.
4. Enter "M" to "Require Multi-Factor Authentication".
5. Enter "E" to "Enable Require Multi-factor Authentication".

Additional Information:

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

1.9 TANS-OS-000330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must use multifactor authentication for network access to nonprivileged accounts.

```
GROUP ID: V-254848
RULE ID: SV-254848r986547
```

Rationale:

To assure accountability and prevent unauthenticated access, nonprivileged users must utilize multifactor authentication to prevent potential misuse and compromise of the system.

Multifactor authentication uses two or more factors to achieve authentication.

Factors include:(i) Something you know (e.g., password/PIN); (ii) Something you have (e.g., cryptographic identification device, token); or (iii) Something you are (e.g., biometric).

A nonprivileged account is any information system account with authorizations of a nonprivileged user.

Network access is any access to an application by a user (or process acting on behalf of a user) where said access is obtained through a network connection.

The DOD CAC with DOD-approved PKI is an example of multifactor authentication.

Audit:

1. Sign in to the TanOS console as a user with the tanadmin role.
2. Enter "C" to go to the "User Administration" menu.
3. Enter "M" to go to the "Multi-Factor Global Settings" menu.
4. If the status shows "Multi-Factor: Optional", this is a finding.

Remediation:

1. Sign in to the TanOS console as a user with the tanadmin role.
2. Enter "C" to go to the "User Administration" menu.
3. Enter "M" to go to the "Multi-Factor Global Settings" menu.
4. Enter "M" to "Require Multi-Factor Authentication".
5. Enter "E" to "Enable Require Multi-factor Authentication".

Additional Information:

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

1.10 TANS-OS-000385 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must use FIPS-validated SHA-2 or higher hash function to protect the integrity of hash message authentication code (HMAC), Key Derivation Functions (KDFs), Random Bit Generation, and hash-only applications.

```
GROUP ID: V-254849
RULE ID: SV-254849r971535
```

Rationale:

To protect the integrity of the authenticator and authentication mechanism used for the cryptographic module used by the network device, the application, operating system, or protocol must be configured to use one of the following hash functions for hashing the password or other authenticator in accordance with SP 800-131Ar1: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, and SHA3-512.

This requirement also include HMAC, KDFs, Random Bit Generation, and hash-only applications (e.g., hashing passwords and use for compute a checksum). For digital signature verification, SP800-131Ar1 allows SHA-1 for legacy use only, but this is discouraged by DOD.

Separate requirements for configuring applications and protocols used by each product (e.g., SNMPv3, SSH, NTP, and other protocols and applications that require server/client authentication) are required to implement this requirement.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press "X" for "Advanced Security," and then press "Enter".

If the FIPS 140-2 setting is currently disabled or persistently disabled, this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press "X" for "Advanced Security," and then press "Enter".
6. Press "1" for "FIPS 140-2 mode (disabled/enabled)".
7. Type "yes" to confirm enabling FIPS 140-2 Mode and then press "Enter".
8. Press "Enter" at the confirmation prompt that instructs the user to reboot the appliance.
9. Type "RR" and press "Enter" to return to the root menu.
10. Press "B" for "Appliance Maintenance," and then press "Enter".
11. Press "B" for "Reboot/Shutdown," and then press "Enter".
12. Press "1" for "Reboot the appliance," and then press "Enter".
13. Type "Yes", and then press "Enter" to reboot the appliance and complete the configuration.

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.11 TANS-OS-000455 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service (DoS) attacks.

```
GROUP ID: V-254851
RULE ID: SV-254851r1067742
```

Rationale:

DoS is a condition that occurs when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

Managing excess capacity ensures sufficient capacity is available to counter flooding attacks. Employing increased capacity and service redundancy may reduce the susceptibility to some DoS attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

Audit:

1. Sign in to the TanOS console as a user with the tanadmin role.
2. Enter "A" to go to the "Appliance Configuration" menu.
3. Enter "A" to go to the "Security" menu.
4. Enter "X" to go to the "Advanced Security" menu.
5. If you see "DOS protection: disabled" in the middle of the screen, this is a finding.

Remediation:

1. Sign in to the TanOS console as a user with the tanadmin role.
2. Enter "A" to go to the "Appliance Configuration" menu.
3. Enter "A" to go to the "Security" menu.
4. Enter "X" to go to the "Advanced Security" menu.
5. Enter "6" to enable DoS protection. The screen updates with an enabled status.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.12 TANS-OS-000465 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Operating System (TanOS) must terminate all network connections associated with a communications session at the end of the session, or as follows: For in-band management sessions (privileged sessions), the session must be terminated after 10 minutes of inactivity; for user sessions (nonprivileged session), the session must be terminated after 15 minutes of inactivity, except to fulfill documented and validated mission requirements.

```
GROUP ID: V-254852
RULE ID: SV-254852r970703
```

Rationale:

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 element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, and de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press "X" for "Advanced Security," and then press "Enter".

If the "Menu Timeout" setting is "-" for "Current" or "Persistent", this is a finding.
If the "Menu Timeout" is greater than "600" (seconds) for either "Current" or "Persistent", this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press "X" for "Advanced Security," and then press "Enter".
6. Press "5" for "Set Menu Timeout," and then press "Enter".
7. Enter a timeout value no greater than "600" seconds, and then press "Enter".

The timeout is not applied until a new login session is started.

8. Type "RR" and press "Enter" to return to the root menu.
9. Press "Z" for "Log out," and then press Enter.

The session will disconnect and the menu timeout will be active at next sign in.

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

1.13 TANS-OS-000515 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must use FIPS-validated encryption and hashing algorithms to protect the confidentiality and integrity of operating system configuration and user-generated data stored on the host.

```
GROUP ID: V-254853
RULE ID: SV-254853r958552
```

Rationale:

Confidentiality and integrity protections are intended to address the confidentiality and integrity of system information at rest when it is located on a storage device within the network device or as a component of the network device. This protection is required to prevent unauthorized alteration, corruption, or disclosure of information when not stored directly on the network device.

This requirement addresses the protection of user-generated data as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press "X" for "Advanced Security," and then press "Enter".

If the FIPS 140-2 setting is currently disabled or persistently disabled, this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press "X" for "Advanced Security," and then press "Enter".
6. Press "1" for "FIPS 140-2 mode (disabled/enabled).
7. Type "yes" to confirm enabling FIPS 140-2 Mode, and then press "Enter".
8. Press "Enter" at the confirmation prompt that instructs the user to reboot the appliance.
9. Type "RR" and press "Enter" to return to the root menu.
10. Press "B" for "Appliance Maintenance," and then press "Enter".
11. Press "B" for "Reboot/Shutdown," and then press "Enter".
12. Press "1" for "Reboot the appliance," and then press "Enter".
13. Type "Yes" and press "Enter" to reboot the appliance and complete the configuration.

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.14 TANS-OS-000535 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must notify the ISSO and ISSM of failed security verification tests.

```
GROUP ID: V-254854
RULE ID: SV-254854r958558
```

Rationale:

If personnel are not notified of failed security verification tests, they will not be able to take corrective action and the unsecure condition(s) will remain. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Notifications provided by information systems include electronic alerts, messages to local computer consoles, and/or hardware indications, such as lights.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and press then "Enter".
4. Press "1" for "Check current status," and then press "Enter".

If the syslog status page states, "No existing TanOS syslog forwarding configuration found", this is a finding.
If the syslog status page states, "Syslog forwarding configuration" and the SIEM administrator verifies SIEM is receiving the events correctly and generating notifications for failed security verification tests, this is not a finding.

Remediation:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "5" for "Configure syslog forwarding," and then press "Enter".
5. Enter the destination host (IP address or hostname) provided by the SIEM administrator, and press "Enter".
6. Enter the destination port number, and then press "Enter".
7. If TLS is required for this syslog destination, enter "Yes", otherwise enter "No", and then press "Enter".
8. Enter the destination protocol, "udp" or "tcp", and then press "Enter".
9. Work with the SIEM administrator to validate events are being received, and to configure notifications for failure events.

Additional Information:

CCI-001294 Alert organization-defined personnel or roles of failed security verification tests.

- NIST SP 800-53::SI-6 (1)
- NIST SP 800-53A::SI-6 (1).1
- NIST SP 800-53 Revision 4::SI-6 c
- NIST SP 800-53 Revision 5::SI-6 c

1.15 TANS-OS-000605 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The publicly accessible Tanium Operating System (TanOS) must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system.

```
GROUP ID: V-254855
RULE ID: SV-254855r958586
```

Rationale:

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060. Use the following verbiage for operating system that can accommodate banners of 1300 characters: "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."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner: "I've read & consent to terms in IS user agreem't".

Audit:

1. Access the TanOS interactively.

If the Standard Mandatory DOD Notice and Consent Banner is not displayed at logon, this is a finding.

Remediation:

1. Use SFTP to copy a file named "banner_ssh.txt" containing the Standard Mandatory DOD Notice and Consent Banner to the /incoming folder.
2. Access the TanOS interactively.
3. Enter "A" to go to the "Appliance Configuration" menu.
4. Enter "A" to go to the "Security" menu.
5. Enter "3" to add the banner file.

Additional Information:

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (iii)
- NIST SP 800-53 Revision 4::AC-8 c 3
- NIST SP 800-53 Revision 5::AC-8 c 3

1.16 TANS-OS-000710 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must notify system administrators (SAs) and information system security officers (ISSOs) when accounts are created.

```
GROUP ID: V-254856
RULE ID: SV-254856r1015854
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create a new account. Notification of account creation is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail which documents the creation of operating system user accounts and notifies administrators and ISSOs that it exists. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and press then "Enter".
4. Press "1" for "Check current status," and then press "Enter".

If the syslog status page states, "No existing TanOS syslog forwarding configuration found", this is a finding.
If the syslog status page states, "Syslog forwarding configuration" and the SIEM administrator verifies SIEM is receiving the events correctly and generating notifications for account creation events, this is not a finding.

Remediation:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "5" for "Configure syslog forwarding," and then press "Enter".
5. Enter the destination host (IP address or hostname) provided by the SIEM administrator, and then press "Enter".
6. Enter the destination port number, and then press "Enter".
7. If TLS is required for this syslog destination, enter "Yes", otherwise enter "No", and then press "Enter".
8. Enter the destination protocol, "udp" or "tcp", and press "Enter".
9. Work with the SIEM administrator to validate events are being received, and to configure notifications for account creation events.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-001683 The information system notifies organization-defined personnel or roles for account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)

1.17 TANS-OS-000715 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must audit and notify system administrators (SAs) and information system security officers (ISSOs) when accounts are modified.

```
GROUP ID: V-254857
RULE ID: SV-254857r1015855
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to modify an existing account. Notification of account modification is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail, which documents the modification of operating system user accounts and notifies the SA and ISSO of changes. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "1" for "Check current status," and then press "Enter".

If the syslog status page states, "No existing TanOS syslog forwarding configuration found", this is a finding.
If the syslog status page states, "Syslog forwarding configuration", and the SIEM administrator verifies SIEM is receiving the events correctly and generating notifications for account modification events, this is not a finding.

Remediation:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "5" for "Configure syslog forwarding," and then press "Enter".
5. Enter the destination host (IP address or hostname) provided by the SIEM administrator, and then press "Enter".
6. Enter the destination port number, and then press "Enter".
7. If TLS is required for this syslog destination, enter "Yes", otherwise enter "No", and then press "Enter".
8. Enter the destination protocol, "udp" or "tcp", and then press "Enter".
9. Work with the SIEM administrator to validate events are being received, and to configure notifications for account modification events.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-001684 The information system notifies organization-defined personnel or roles for account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)

1.18 TANS-OS-000725 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must notify system administrators (SAs) and information system security officers (ISSOs) when accounts are removed.

```
GROUP ID: V-254858
RULE ID: SV-254858r1015856
```

Rationale:

When operating system accounts are removed, user accessibility is affected. Accounts are utilized for identifying individual operating system users or for identifying the operating system processes themselves. Sending notification of account removal events to the SA and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "1" for "Check current status," and then press "Enter".

If the syslog status page states "No existing TanOS syslog forwarding configuration found" this is a finding.
If the syslog status page states "Syslog forwarding configuration" and the SIEM administrator verifies SIEM is receiving the events correctly and generating notifications for account removal events, this is not a finding.

Remediation:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "5" for "Configure syslog forwarding," and press then "Enter".
5. Enter the destination host (IP address or hostname) provided by the SIEM administrator, and then press "Enter".
6. Enter the destination port number and press "Enter".
7. If TLS is required for this syslog destination, enter "Yes", otherwise enter "No", and then press "Enter".
8. Enter the destination protocol, "udp" or "tcp", and press "Enter".
9. Work with the SIEM administrator to validate events are being received, and to configure notifications for account removal/deletion events.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-001686 The information system notifies organization-defined personnel or roles for account removal actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)

1.19 TANS-OS-000735 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Operating System (TanOS) must automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

```
GROUP ID: V-254859
RULE ID: SV-254859r958636
```

Rationale:

Automatic session termination addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.

Audit:

1. Sign in to the TanOS console as a user with the tanadmin role.
2. Enter "A" to go to the "Appliance Configuration" menu.
3. Enter "A" to go to the "Security" menu.
4. Enter "X" to go to the "Advanced Security" menu.
5. Enter "5" to go to "Set Menu Timeout".
6. See the current setting for timeout, if this does not match the organizationally defined standard, this is a finding.

Remediation:

1. Sign in to the TanOS console as a user with the tanadmin role.
2. Enter "A" to go to the "Appliance Configuration" menu.
3. Enter "A" to go to the "" menu.
4. Enter "X" to go to the "Advanced Security" menu.
5. Enter "5" to go to "Set Menu Timeout".
6. Enter the correct Timeout in seconds, and then press "Enter" to set the setting.

Additional Information:

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

1.20 TANS-OS-000860 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must audit and notify system administrators (SAs) and information system security officers (ISSOs) when accounts are enabled.

```
GROUP ID: V-254860
RULE ID: SV-254860r1015857
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to enable an existing disabled account. Sending notification of account enabling actions to the SA and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To detect and respond to events that affect user accessibility and application processing, operating systems must audit account enabling actions and, as required, notify the appropriate individuals so they can investigate the event.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Access the Tanium Operating System (TanOS) interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "1" for "Check current status," and then press "Enter".

If the syslog status page states, "No existing TanOS syslog forwarding configuration found", this is a finding.
If the syslog status page states, "Syslog forwarding configuration" and the SIEM administrator verifies SIEM is receiving the events correctly and generating notifications for account enable events, this is not a finding.

Remediation:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "5" for "Configure syslog forwarding," and then press "Enter".
5. Enter the destination host (IP address or hostname) provided by the SIEM administrator, and then press "Enter".
6. Enter the destination port number and then press "Enter".
7. If TLS is required for this syslog destination, enter "Yes", otherwise enter "No", and then press "Enter".
8. Enter the destination protocol, "udp" or "tcp", and then press "Enter".
9. Work with the SIEM administrator to validate events are being received, and to configure notifications for account removal/deletion events.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

1.21 TANS-OS-000985 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must automatically lock accounts and require them be unlocked by an administrator when three unsuccessful login attempts in 15 minutes are exceeded.

```
GROUP ID: V-254861
RULE ID: SV-254861r1067744
```

Rationale:

By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Audit:

1. Log in to Tanium interactively as a TanAdmin user.
2. Type "A" for "Appliance Configuration Menu".
3. Type "A" for Security.
4. Type "P" for Security Policy.
5. The section for "Account lockout:" should read "0 seconds after 3 failures".

If the section reads anything else, this is a finding.

Remediation:

1. Log in to Tanium interactively as a TanAdmin user.
2. Type "A" for "Appliance Configuration Menu".
3. Type "A" for "Security".
4. Type "P" for "Security Policy".
5. Type "L" for "Account Lockout Time".
6. Set the account lockout time to "0".

Note: The time range for the three failures to occur is 15 minutes by default and cannot be configured otherwise.

Additional Information:

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

1.22 TANS-OS-001030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium operating system (TanOS) must offload audit records onto a different system or media than the system being audited.

```
GROUP ID: V-254862
RULE ID: SV-254862r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342, SRG-OS-000479, SRG-OS-000215, SRG-OS-000062

Audit:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "1" for "Check current status," and then press "Enter".

If the syslog status page states "No existing TanOS syslog forwarding configuration found" this is a finding.
If the syslog status page states "Syslog forwarding configuration" and the SIEM administrator verifies that the destination SIEM is receiving the events correctly, this is not a finding.

Remediation:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "5" for "Configure syslog forwarding," and then press "Enter".
5. Enter the destination host (IP address or hostname) provided by the SIEM administrator, and then press "Enter".
6. Enter the destination port number and press "Enter".
7. If TLS is required for this syslog destination, enter "Yes", otherwise enter "No", and then press "Enter".
8. Enter the destination protocol, "udp" or "tcp", and then press "Enter".
9. Work with the SIEM administrator to validate events are being received.

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

1.23 TANS-OS-001035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium operating system (TanOS) must provide an immediate warning to the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity.

```
GROUP ID: V-254863
RULE ID: SV-254863r971542
```

Rationale:

If security personnel are not notified immediately when storage volume reaches 75 percent, they are unable to plan for audit record storage capacity expansion.

Audit:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "5" for "SNMP Configuration," and then press "Enter".

If the State is "Disabled" this is a finding.
If the state is "Enabled", work with the SNMP monitoring system administrator to ensure warnings are sent when TanOS storage reaches 75 percent of capacity. If they are not being sent, and this is a finding.

Remediation:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "5" for "SNMP Configuration," and then press "Enter".
4. Press "S" for "Set Password and Start the SNMP Service," and then press "Enter".
5. Enter the desired SNMP password and press "Enter".
6. Press "Enter" to continue and return to the SNMP configuration menu and verify the state is now "Enabled".

Work with the SNMP monitoring system administrator to enable warning alerts for low free space.

Additional Information:

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4::AU-5 (1)
- NIST SP 800-53 Revision 5::AU-5 (1)

1.24 TANS-OS-001040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium operating system (TanOS) must provide an immediate real-time alert to the SA and ISSO, at a minimum, of all audit failure events requiring real-time alerts.

```
GROUP ID: V-254864
RULE ID: SV-254864r958758
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of an impending failure of the audit capability and system operation may be adversely affected.

Alerts provide organizations with urgent messages. Real-time alerts provide these messages immediately (i.e., the time from event detection to alert occurs in seconds or less).

Audit:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "1" for "Check current status," and then press "Enter".

If the syslog status page states "No existing TanOS syslog forwarding configuration found" this is a finding.
If the syslog status page states "Syslog forwarding configuration" and the SIEM administrator verifies SIEM is receiving the events correctly and generating notifications for audit failure events, this is not a finding.

Remediation:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "5" for "Configure syslog forwarding," and then press "Enter".
5. Enter the destination host (IP address or hostname) provided by the SIEM administrator, and then press "Enter".
6. Enter the destination port number and press "Enter".
7. If TLS is required for this syslog destination, enter "Yes", otherwise enter "No", and press "Enter".
8. Enter the destination protocol, "udp" or "tcp", and press "Enter".
9. Work with the SIEM administrator to validate events are being received, and to configure notifications for audit failure events.

Additional Information:

CCI-001858 Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

- NIST SP 800-53 Revision 4::AU-5 (2)
- NIST SP 800-53 Revision 5::AU-5 (2)

1.25 TANS-OS-001095 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium operating system (TanOS) must, for networked systems, compare internal information system clocks at least every 24 hours with a server synchronized to one of the redundant United States Naval Observatory (USNO) time servers or a time server designated for the appropriate DOD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

```
GROUP ID: V-254865
RULE ID: SV-254865r1067747
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside of the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "3" for "NTP Configuration," and then press "Enter".

If there is no address listed for "Currently configured ntp servers:", this is a finding.
The status is reported differently in different versions of TanOS.
TanOS <= 1.7.1:
If the "Current NTP Status" does not list a status of "Synchronized to NTP Server (
) at stratum #" and "Time correct to within # ms", this is a finding.
TanOS >= 1.7.2:
If the "Current NTP Status" does not list a status of "Normal", this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "3" for "NTP Configuration," and then press "Enter".
5. Type "Yes" to "Remove the current NTP servers and enter new information?" and then press "Enter".
6. Type the first NTP server address and then press "Enter".
7. Type "Yes" to provide a second NTP Server, and then press "Enter".
8. Type the second NTP server address and then press "Enter".
9. Press "Enter" to return to the "Appliance Configuration" menu.

Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (1) (a)

1.26 TANS-OS-001100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must synchronize internal information system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

```
GROUP ID: V-254866
RULE ID: SV-254866r1067750
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. Organizations must consider setting time periods for different types of systems (e.g., financial, legal, or mission-critical systems).

Organizations should also consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints). This requirement is related to the comparison done every 24 hours in CCI-001891 because a comparison must be done to determine the time difference.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "3" for "NTP Configuration," and then press "Enter".

If there is no address listed for "Currently configured ntp servers:", this is a finding.
The status is reported differently in different versions of TanOS.
TanOS <= 1.7.1:
If the "Current NTP Status" does not list a status of "Synchronized to NTP Server (
) at stratum #" and "Time correct to within # ms", this is a finding.
TanOS >= 1.7.2:
If the "Current NTP Status" does not list a status of "Normal", this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "3" for "NTP Configuration," and then press "Enter".
5. Type "Yes" to "Remove the current NTP servers and enter new information?" and then press "Enter".
6. Type the first NTP server address and then press "Enter".
7. Type "Yes" to provide a second NTP Server, and then press "Enter".
8. Type the second NTP server address and then press "Enter".
9. Press "Enter" to return to the "Appliance Configuration" menu.

Additional Information:

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

CCI-002046 The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

- NIST SP 800-53 Revision 4::AU-8 (1) (b)

1.27 TANS-OS-001105 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Operating System (TanOS) must be configured to synchronize internal information system clocks with the primary and secondary time sources located in different geographic regions using redundant authoritative time sources.

```
GROUP ID: V-254867
RULE ID: SV-254867r1015860
```

Rationale:

The loss of connectivity to a particular authoritative time source will result in the loss of time synchronization (free-run mode) and increasingly inaccurate time stamps on audit events and other functions.

Multiple time sources provide redundancy by including a secondary source. Time synchronization is usually a hierarchy; clients synchronize time to a local source while that source synchronizes it's time to a more accurate source. The system must utilize an authoritative time server and/or be configured to use redundant authoritative time sources. Organizations should also consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints). This requirement is related to the comparison done in CCI-001891.

DOD-approved solutions consist of a combination of a primary and secondary time source using a combination or multiple instances of the following: A time server designated for the appropriate DOD network (NIPRNet/SIPRNet); United States Naval Observatory (USNO) time servers; and/or the Global Positioning System (GPS). The secondary time source must be located in a different geographic region than the primary time source.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "3" for "NTP Configuration," and then press "Enter".

If there is no address or only a single address listed for "Currently configured ntp servers:", this is a finding.
If the "Currently configured ntp servers:" list is not the organizationally mandated list of geographically distributed time servers, this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "3" for "NTP Configuration," and then press "Enter".
5. Type "Yes" to "Remove the current NTP servers and enter new information?" and press "Enter".
6. Type the first NTP server address and press "Enter".
7. Type "Yes" to provide a second NTP Server, and then press "Enter".
8. Type the second NTP server address, and then press "Enter".
9. Press "Enter" to return to the "Appliance Configuration" menu.

Additional Information:

CCI-004928 Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (2) (a)

CCI-001893 The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (2)

1.28 TANS-OS-001325 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium operating system (TanOS) must perform data integrity verification on the name/address resolution responses the system receives from authoritative sources.

```
GROUP ID: V-254868
RULE ID: SV-254868r958864
```

Rationale:

If data origin authentication and data integrity verification is not performed, the resultant response could be forged, it may have come from a poisoned cache, the packets could have been intercepted without the resolver's knowledge, or resource records could have been removed, which would result in query failure or denial of service. Data integrity verification must be performed to thwart these types of attacks.

Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching Domain Name System (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations.

This applies to operating systems that have integrated DNS clients.

Audit:

1. Work with a systems administrator to determine a designated Name Server that performs data integrity checks.
2. Sign in to the TanOS console as a user with the tanadmin role.
3. Enter "A" to go to the "Appliance Configuration" menu.
4. Enter "1" to go to the "Hostname/DNS Configuration" menu.
5. Enter "2", if the ip address shown is not the designated Name Server determined in step 1. This is a finding.

Remediation:

1. Work with a systems administrator to determine a designated Name Server that performs data integrity checks.
2. Sign in to the TanOS console as a user with the tanadmin role.
3. Enter "A" to go to the "Appliance Configuration" menu.
4. Enter "1" to go to the "Hostname/DNS Configuration" menu.
5. Enter "2" and follow the prompts to modify the DNS server configuration.

Additional Information:

CCI-002467 Perform data integrity verification on the name/address resolution responses the system receives from authoritative sources.

- NIST SP 800-53 Revision 4::SC-21
- NIST SP 800-53 Revision 5::SC-21

1.29 TANS-OS-001330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium operating system (TanOS) must perform data origin verification authentication on the name/address resolution responses the system receives from authoritative sources.

```
GROUP ID: V-254869
RULE ID: SV-254869r958866
```

Rationale:

If data origin authentication and data integrity verification is not performed, the resultant response could be forged, it may have come from a poisoned cache, the packets could have been intercepted without the resolver's knowledge, or resource records could have been removed, which would result in query failure or denial of service. Data origin authentication verification must be performed to thwart these types of attacks.

Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching Domain Name System (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations.

This applies to operating systems that have integrated DNS clients.

Audit:

1. Work with a systems administrator to determine a designated Name Server that performs data origin authentic ion checks.
2. Sign in to the TanOS console as a user with the tanadmin role.
3. Enter "A" to go to the "Appliance Configuration" menu.
4. Enter "1" to go to the "Hostname/DNS Configuration" menu.
5. Enter "2", if the ip address shown is not the designated Name Server determined in step 1. This is a finding.

Remediation:

1. Work with a systems administrator to determine a designated Name Server that performs data origin authentic ion checks.
2. Sign in to the TanOS console as a user with the tanadmin role.
3. Enter "A" to go to the "Appliance Configuration" menu.
4. Enter "1" to go to the "Hostname/DNS Configuration" menu.
5. Enter "2" and follow the prompts to modify the DNS server configuration.

Additional Information:

CCI-002468 Perform data origin verification authentication on the name/address resolution responses the system receives from authoritative sources.

- NIST SP 800-53 Revision 4::SC-21
- NIST SP 800-53 Revision 5::SC-21

1.30 TANS-OS-001515 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium operating system (TanOS) must install security-relevant software updates within the time period directed by an authoritative source (e.g., IAVM, CTOs, DTMs, and STIGs).

```
GROUP ID: V-254871
RULE ID: SV-254871r958940
```

Rationale:

Security flaws with operating systems are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations (including any contractor to the organization) are required to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

Organization-defined time periods for updating security-relevant software may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw).

Patch criticality, as well as system criticality will vary. Therefore, the tactical situations regarding the patch management process will also vary. This means that the time period utilized must be a configurable parameter. Time frames for application of security-relevant software updates may be dependent upon the Information Assurance Vulnerability Management (IAVM) process.

The application will be configured to check for and install security-relevant software updates within an identified time period from the availability of the update. The specific time period will be defined by an authoritative source (e.g. IAVM, CTOs, DTMs, and STIGs).

Audit:

1. Access the Tanium Server interactively.
2. Check the version number of the installed TanOS release displayed at the bottom of the main menu.
3. Compare to the latest available release on https://kb.tanium.com/Category:TanOS.
4. If the installed release is not the current release, review the release notes for the current release and any other releases newer than the current version to check for security-relevant updates and when they were released.

If there are security-relevant updates that have not been installed within the directed time period, this is a finding.

Remediation:

1. Download the target TanOS upgrade file from Tanium.
2. Transfer the upgrade to the SFTP incoming folder on the TanOS appliance.
3. Access the Tanium Server interactively.
4. Press "B" for "Appliance Maintenance Menu," and then press "Enter".
5. Press "3" for "Upgrade TanOS," and then press "Enter".

5b. If this TanOS server is part of an appliance array, type "yes" and then press "Enter" to choose to upgrade all appliances in the array.

6. Press "1" (or the appropriate number if there are multiple upgrade files to select from) to choose the upgrade file to install.
7. Review the upgrade version confirmation and type "Yes" and then press "Enter" to begin the upgrade.

Additional Information:

CCI-002605 Install security-relevant software updates within an organization-defined time period of the release of the updates.

- NIST SP 800-53 Revision 4::SI-2 c
- NIST SP 800-53 Revision 5::SI-2 c

1.31 TANS-OS-001760 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Tanium Operating System (TanOS) must use a FIPS-validated cryptographic module to provision digital signatures.

```
GROUP ID: V-254873
RULE ID: SV-254873r959036
```

Rationale:

FIPS 140-2 precludes the use of invalidated cryptography for the cryptographic protection of sensitive or valuable data within federal systems. Un-validated cryptography is viewed by NIST as providing no protection to the information or data - in effect the data would be considered unprotected plaintext. If the agency specifies that the information or data be cryptographically protected, then FIPS 140-2 is applicable. In essence, if cryptography is required, then it must be validated. Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against the FIPS 140-2 standard.

The cryptographic module used must have at least one validated digital signature function. This validated hash algorithm must be used to generate digital signatures for all cryptographic security function within the product being evaluated.

Satisfies: SRG-OS-000550, SRG-OS-000530

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press "X" for "Advanced Security," and then press "Enter".

If the FIPS 140-2 setting is currently disabled or persistently disabled, this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "A" for "Appliance Configuration Menu," and then press "Enter".
4. Press "A" for "Security," and then press "Enter".
5. Press "X" for "Advanced Security," and then press "Enter".
6. Press "1" for "FIPS 140-2 mode (disabled/enabled)".
7. Type "yes" to confirm enabling FIPS 140-2 Mode, and then press "Enter".
8. Press "Enter" at the confirmation prompt that instructs the user to reboot the appliance.
9. Type "RR" and press "Enter" to return to the root menu.
10. Press "B" for "Appliance Maintenance," and then press "Enter".
11. Press "B" for "Reboot/Shutdown," and then press "Enter".
12. Press "1" for "Reboot the appliance," and then press "Enter".
13. Type "Yes" and then press "Enter" to reboot the appliance and complete the configuration.

Additional Information:

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	TANS-OS-000070 (Manual)	☐	☐
1.2	TANS-OS-000075 (Manual)	☐	☐
1.3	TANS-OS-000095 (Manual)	☐	☐
1.4	TANS-OS-000165 (Manual)	☐	☐
1.5	TANS-OS-000270 (Manual)	☐	☐
1.6	TANS-OS-000275 (Manual)	☐	☐
1.7	TANS-OS-000285 (Manual)	☐	☐
1.8	TANS-OS-000325 (Manual)	☐	☐
1.9	TANS-OS-000330 (Manual)	☐	☐
1.10	TANS-OS-000385 (Manual)	☐	☐
1.11	TANS-OS-000455 (Manual)	☐	☐
1.12	TANS-OS-000465 (Manual)	☐	☐
1.13	TANS-OS-000515 (Manual)	☐	☐
1.14	TANS-OS-000535 (Manual)	☐	☐
1.15	TANS-OS-000605 (Manual)	☐	☐
1.16	TANS-OS-000710 (Manual)	☐	☐
1.17	TANS-OS-000715 (Manual)	☐	☐
1.18	TANS-OS-000725 (Manual)	☐	☐
1.19	TANS-OS-000735 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	TANS-OS-000860 (Manual)	☐	☐
1.21	TANS-OS-000985 (Manual)	☐	☐
1.22	TANS-OS-001030 (Manual)	☐	☐
1.23	TANS-OS-001035 (Manual)	☐	☐
1.24	TANS-OS-001040 (Manual)	☐	☐
1.25	TANS-OS-001095 (Manual)	☐	☐
1.26	TANS-OS-001100 (Manual)	☐	☐
1.27	TANS-OS-001105 (Manual)	☐	☐
1.28	TANS-OS-001325 (Manual)	☐	☐
1.29	TANS-OS-001330 (Manual)	☐	☐
1.30	TANS-OS-001515 (Manual)	☐	☐
1.31	TANS-OS-001760 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 22, 2025	1.0.0	Initial CIS Release