CIS Xylok Security Suite 20.x STIG Benchmark

v1.0.0 – 12-10-2024

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

Xylok Security Suite 20.x Secure Technical Implementation Guide (STIG)
Version: 1 Release: 1 Benchmark
Date: 10 Dec 2024

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 Xylok Security Suite 20.x and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

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 Xylok Security Suite 20.x

Recommendations

1 STIG RULES

Xylok Security Suite 20.x

Xylok Security Suite 20.x Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 10 Dec 2024

CLASSIFICATION unclassified

1.1 XYLK-20-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must limit system resources consumed by the application.

```
GROUP ID: V-269570
RULE ID: SV-269570r1053485
```

Rationale:

Not limiting system resources to Xylok presents a denial-of-service (DoS) risk. Each open instance of Xylok periodically retrieves a list of background tasks. Open sessions, even sessions not being actively used, consume a small amount of server resources and could result in Xylok becoming slow or entirely responsive.

In addition, this risk impacts the host system for the container by consuming excessive CPU, allowing a DoS attack on Xylok to also impact other software hosted on the same physical machine.

Satisfies: SRG-APP-000001, SRG-APP-000435

Audit:

Determine if Xylok is configured to limit its maximum CPU and memory usage with the following command, run from the host machine as a normal user:

```
$ grep LIMIT_ /etc/xylok.conf
```

Verify the following settings are configured:

- LIMIT_MEM set to less than 100 percent of the host machine's memory.
- LIMIT_CPU set to less than 1000.

If any of the above settings are not present or are blank, this is a finding.

Remediation:

Configure the Xylok Security Suite to limit CPU and memory usage using this procedure on the host machine. As root, open /etc/xylok.conf in a text editor.

1. Add the following settings if not present. All settings should be in the format "NAME=value". For example, the first required setting might appear as "LIMIT_MEM=4096m" in the configuration file, with no quotes.

- LIMIT_MEM: Set to 2048m or greater, and less than 100 percent of the host machine's memory.
- LIMIT_CPU: Set to 128 or greater, not to exceed 1000. This value can range from 1 to 1024, where 1024 allows usage of 100 percent of the CPU.

2. Save configuration file.
3. Restart Xylok to apply settings:

systemctl restart xylok

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

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

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

1.2 XYLK-20-000003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must initiate a session lock after a 15-minute period of inactivity.

```
GROUP ID: V-269571
RULE ID: SV-269571r1053488
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system, but does not log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined and/or controlled. This is handled at the operating system-level and results in a system lock.

Satisfies: SRG-APP-000003, SRG-APP-000190

Audit:

Verify session is configured to lock after 15 minutes of inactivity. Execute the following:

```
$ grep SESSION_LENGTH /etc/xylok.conf
```

SESSION_LENGTH=900
If "SESSION_LENGTH" is set to more than15 minutes or is missing, this is a finding.
Note: The setting is in seconds. 900 sec = 15 min.

Remediation:

Set the session length:

1. As root, open /etc/xylok.conf in a text editor.
2. Add/Amend "SESSION_LENGTH=900" to the configuration file.
3. Restart Xylok to apply settings by executing the following:

```
systemctl restart xylok
```

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

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

1.3 XYLK-20-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Xylok Security Suite must expire a session upon browser closing.

```
GROUP ID: V-269572
RULE ID: SV-269572r1053491
```

Rationale:

When the session expires as soon as the browser is closed, it prevents session hijacking and unauthorized users from accessing the account or data if they reopen the browser.

Leaving a session open in the browser even after it is closed could expose the system to various types of attacks, like cross-site scripting (XSS) or malware designed to steal session cookies. Automatically expiring sessions mitigates this risk.

Satisfies: SRG-APP-000005, SRG-APP-000220, SRG-APP-000295, SRG-APP-000413

Audit:

Verify session expires after browser is closed. Execute the following:

```
$ grep SESSION_EXPIRE_AT_BROWSER_CLOSE /etc/xylok.conf
```

SESSION_EXPIRE_AT_BROWSER_CLOSE=True
If "SESSION_EXPIRE_AT_BROWSER_CLOSE" is not set to "True" or is missing, this is a finding.

Remediation:

Set the session expiration:

1. As root, open /etc/xylok.conf in a text editor.
2. Add/Amend "SESSION_EXPIRE_AT_BROWSER_CLOSE=True" to the configuration file.
3. Restart Xylok to apply settings by executing the following:

systemctl restart xylok

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

CCI-001185 Invalidate session identifiers upon user logout or other session termination.

- NIST SP 800-53::SC-23 (1)
- NIST SP 800-53A::SC-23 (1).1
- NIST SP 800-53 Revision 4::SC-23 (1)
- NIST SP 800-53 Revision 5::SC-23 (1)

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

CCI-002891 Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (7)
- NIST SP 800-53 Revision 5::MA-4 (7)

1.4 XYLK-20-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Xylok Security Suite must prevent access except through HTTPS.

```
GROUP ID: V-269573
RULE ID: SV-269573r1054093
```

Rationale:

Preventing access, except via HTTPS, ensures security and protects sensitive data. HTTP_ONLY: If true, disables listening on the HTTPS port and allows all calls to happen over HTTP. This must be set to false. HTTPS encrypts data transmitted between the client (browser) and the server. Sensitive information, such as login credentials, personal data, and session cookies, is protected from being intercepted by malicious actors (e.g., through man-in-the-middle attacks) during transmission. When data is sent over HTTP (unencrypted), it can be intercepted and altered. HTTPS mitigates this by encrypting the communication. HTTPS uses digital certificates (SSL/TLS certificates) to authenticate the server's identity. This ensures that users are connecting to the legitimate server rather than a malicious entity attempting to impersonate the site. HTTPS-only policies enable the use of HSTS, which forces browsers to only interact with the site using HTTPS and prevents users from being redirected to an HTTP version of the site. This can defend against certain attacks, like SSL stripping, which downgrade connections to HTTP.

Satisfies: SRG-APP-000014, SRG-APP-000142, SRG-APP-000219, SRG-APP-000411, SRG-APP-000412, SRG-APP-000439, SRG-APP-000440, SRG-APP-000442, SRG-APP-000514, SRG-APP-000555, SRG-APP-000645

Audit:

Verify HTTP_ONLY is set to "false":

```
$ grep HTTP_ONLY
```

/etc/xylok.conf HTTP_ONLY=false
If "HTTP_ONLY=true" or is not configured, this is a finding.

Remediation:

Add/Amend HTTP_ONLY to the configuration files:

1. As root, open /etc/xylok.conf in a text editor.
2. Add/Amend the following to the configuration file:
   HTTP_ONLY=false
3. Restart Xylok to apply settings by executing the following:

systemctl restart xylok

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

CCI-001184 Protect the authenticity of communications sessions.

- NIST SP 800-53::SC-23
- NIST SP 800-53A::SC-23.1
- NIST SP 800-53 Revision 4::SC-23
- NIST SP 800-53 Revision 5::SC-23

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

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

1.5 XYLK-20-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Xylok Security Suite must use a centralized user management solution.

```
GROUP ID: V-269574
RULE ID: SV-269574r1053497
```

Rationale:

Configuring Xylok Security Suite to integrate with an Enterprise Identity Provider enhances security, simplifies user management, ensures compliance, provides auditing capabilities, and offers a more seamless and consistent user experience. It aligns Xylok Security Suite with enterprise standards and contributes to a more efficient and secure environment.

Satisfies: SRG-APP-000023, SRG-APP-000025, SRG-APP-000026, SRG-APP-000027, SRG-APP-000028, SRG-APP-000029, SRG-APP-000033, SRG-APP-000065, SRG-APP-000080, SRG-APP-000089, SRG-APP-000090, SRG-APP-000149, SRG-APP-000150, SRG-APP-000153, SRG-APP-000154, SRG-APP-000155, SRG-APP-000156, SRG-APP-000157, SRG-APP-000163, SRG-APP-000164, SRG-APP-000165, SRG-APP-000166, SRG-APP-000167, SRG-APP-000168, SRG-APP-000169, SRG-APP-000170, SRG-APP-000173, SRG-APP-000175, SRG-APP-000176, SRG-APP-000177, SRG-APP-000180, SRG-APP-000185, SRG-APP-000291, SRG-APP-000292, SRG-APP-000293, SRG-APP-000294, SRG-APP-000318, SRG-APP-000319, SRG-APP-000320, SRG-APP-000345, SRG-APP-000391, SRG-APP-000392, SRG-APP-000401, SRG-APP-000402, SRG-APP-000403, SRG-APP-000404, SRG-APP-000405, SRG-APP-000503, SRG-APP-000505, SRG-APP-000506, SRG-APP-000508, SRG-APP-000700, SRG-APP-000705, SRG-APP-000710, SRG-APP-000815, SRG-APP-000820, SRG-APP-000825, SRG-APP-000830, SRG-APP-000835, SRG-APP-000840, SRG-APP-000845, SRG-APP-000850, SRG-APP-000855, SRG-APP-000860, SRG-APP-000865, SRG-APP-000870, SRG-APP-000875, SRG-APP-000910

Audit:

Determine if Xylok is configured to use Active Directory (AD) authentication with the following command, run from the host machine as a normal user:

```
$ grep -e "AD_SIGN_IN" -e "XYLOK_HOST" -e "AD_CLIENT_ID" /etc/xylok.conf
```

Verify the following settings are present:

- AD_SIGN_IN
- XYLOK_HOST
- AD_CLIENT_ID

If any of the above settings are not present, blank, or "false" (case insensitive), this is a finding.

Remediation:

The below procedure assumes an AD server hosted on Windows Server. For AD login using Azure AD, refer to the current Xylok Security Suite manual. Additional advice for AD configuration can also be found in the Xylok manual.
Configure the Xylok Security Suite to use Active Directory login using this procedure on the host machine:

1. As root, open /etc/xylok.conf in a text editor.
2. Add the following settings if not present. All settings should be in the format "NAME=value". For example, the first required setting will appear as "AD_SIGN_IN=True" in the configuration file, with no quotes.

- AD_SIGN_IN: use the value "True"
- XYLOK_HOST: set to domain name used to access server on network
- AD_CLIENT_ID: This is the value displayed on the ADFS server as ClientId when executing the Add-AdfsClient command
- AD_SERVER: The fully qualified domain name (FQDN) of the ADFS server
- AD_AUDIENCE: Set this to the value of the aud claim your ADFS server sends back in the JWT token. If this is a URL, it will be the same as the RELYING_PARTY_ID .
- AD_RELYING_PARTY_ID: Set this to the Relying Party Trust identifier value of the Relying Party Trust (2012) or Web application (2016) configured in ADFS.

3. Save the configuration file.
4. Restart Xylok to apply settings:

systemctl restart xylok

5. In a web browser on a system with access to Xylok, go to https:///oauth2/login. If SSO is configured correctly, it will redirect to the organization's sign-on page.

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-000017 Disable accounts when the accounts have been inactive for the organization-defined time-period.

- NIST SP 800-53::AC-2 (3)
- NIST SP 800-53A::AC-2 (3).1 (ii)
- NIST SP 800-53 Revision 4::AC-2 (3)
- NIST SP 800-53 Revision 5::AC-2 (3) (d)

CCI-000018 Automatically audit account creation 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)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001403 Automatically audit account modification 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)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling 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)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001405 Automatically audit 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)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

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

CCI-000166 Provide irrefutable evidence that an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

- NIST SP 800-53::AU-10
- NIST SP 800-53A::AU-10.1
- NIST SP 800-53 Revision 4::AU-10
- NIST SP 800-53 Revision 5::AU-10

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-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)

- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

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-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-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

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

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

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

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5::AC-2 (3) (a)

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

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

CCI-004061 For password-based authentication, verify when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5 (1) (a).

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

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-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

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

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

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

CCI-000804 Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53::IA-8
- NIST SP 800-53A::IA-8.1
- NIST SP 800-53 Revision 4::IA-8
- NIST SP 800-53 Revision 5::IA-8

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53::MA-4 c
- NIST SP 800-53A::MA-4.1 (iv)
- NIST SP 800-53 Revision 4::MA-4 c
- NIST SP 800-53 Revision 5::MA-4 c

CCI-002145 Enforce organization-defined circumstances and/or usage conditions for organization-defined system accounts.

- NIST SP 800-53 Revision 4::AC-2 (11)
- NIST SP 800-53 Revision 5::AC-2 (11)

CCI-002130 Automatically audit account enabling actions.

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

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

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-001954 Electronically verify Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

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

CCI-002009 Accept Personal Identity Verification-compliant credentials from other federal agencies.

- NIST SP 800-53 Revision 4::IA-8 (1)
- NIST SP 800-53 Revision 5::IA-8 (1)

CCI-002010 Electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

- NIST SP 800-53 Revision 4::IA-8 (1)
- NIST SP 800-53 Revision 5::IA-8 (1)

CCI-004083 Accept only external credentials that are NIST compliant.

- NIST SP 800-53 Revision 5::IA-8 (2) (a)

CCI-004085 Conform to organization-defined identity management profiles for identity management.

- NIST SP 800-53 Revision 5::IA-8 (4)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-003628 Disable accounts when the accounts are no longer associated to a user.

- NIST SP 800-53 Revision 5::AC-2 (3) (b)

CCI-003629 Disable accounts when the accounts are in violation of organizational policy.

- NIST SP 800-53 Revision 5::AC-2 (3) (c)

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)

CCI-004058 For password-based authentication, maintain a list of commonly used, expected, or compromised passwords on an organization-defined frequency.

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

CCI-004059 For password-based authentication, update the list of passwords on an organization-defined frequency.

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

CCI-004060 For password-based authentication, update the list of passwords when organizational passwords are suspected to have been compromised directly or indirectly.

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

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

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

CCI-004063 For password-based authentication, require immediate selection of a new password upon account recovery.

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

CCI-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

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

CCI-004065 For password-based authentication, employ automated tools to assist the user in selecting strong password authenticators.

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

CCI-004909 Include only approved trust anchors in trust stores or certificate stores managed by the organization.

- NIST SP 800-53 Revision 5::SC-17 b

1.6 XYLK-20-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must display the Standard Mandatory DOD Notice and Consent Banner before granting access.

```
GROUP ID: V-269575
RULE ID: SV-269575r1054094
```

Rationale:

Users accessing Xylok must be informed their actions might be monitored, potentially opening the organization up to legal challenges. Implementing a Consent Banner helps Xylok Security Suite remain compliant with legal requirements and protect user privacy while informing users of their rights regarding their data.

Satisfies: SRG-APP-000068, SRG-APP-000069

Audit:

Verify the Standard Mandatory DOD Notice and Consent Banner has been configured:

```
$ grep BANNER /etc/xylok.conf
```

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

Remediation:

Add banner to the configuration files:

1. As root, open /etc/xylok.conf in a text editor.
2. Add/Amend the following to the configuration file:
   BANNER=You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.\nBy using this IS (which includes any device attached to this IS), you consent to the following conditions:\n-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.\n\n- At any time, the USG may inspect and seize data stored on this IS.\n\n- 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.\n\n- This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.\n\n- 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.
3. Restart Xylok to apply settings by executing the following:

systemctl restart xylok

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

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

1.7 XYLK-20-000043 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must protect audit information from any type of unauthorized access.

```
GROUP ID: V-269576
RULE ID: SV-269576r1053503
```

Rationale:

If audit data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity is difficult if not impossible to achieve. In addition, access to audit records provides information an attacker could potentially use to their advantage.

To ensure the veracity of audit data, the information system and/or the Xylok Security Suite must protect audit information from any and all unauthorized access. This includes read, write, and copy access.

Satisfies: SRG-APP-000118, SRG-APP-000119, SRG-APP-000120, SRG-APP-000121, SRG-APP-000122, SRG-APP-000123

Audit:

Check the Xylok log file directory permissions with the following command:

```
$ ls -l /var/log/xylok
```

If any of the directories have permissions greater than "0770", this is a finding.

Remediation:

As root, remove all global permissions for Xylok's log files by running:

chmod -R 0770 /var/log/xylok/

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

1.8 XYLK-20-000051 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Xylok Security Suite must be running a supported version.

```
GROUP ID: V-269577
RULE ID: SV-269577r1053506
```

Rationale:

It is critical to the security and stability of Xylok to ensure that updates and patches are deployed through a trusted software supply chain. Key elements to having a trusted supply chain include ensuring that versions deployed come from known, trusted sources. Additionally, it is important to check for and apply security-relevant updates in a timely manner. To help users manage updates, Xylok manages versions via their internal portal.

Satisfies: SRG-APP-000131, SRG-APP-000456

Audit:

Verify the latest install is being used.
Log on to the GUI and locate the version from the lower left corner.
Compare this version with the latest release on the Xylok portal (https://downloads.xylok.io).
If the current version is not the latest version from the Xylok portal, this is a finding.

Remediation:

Update Xylok Security Suite to the latest version.
Follow the instructions found here: https://app.xylok.io/docs/01-server-admin/installation/updating/.

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

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

1.9 XYLK-20-000052 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Xylok Security Suite READONLY configuration must be True.

```
GROUP ID: V-269578
RULE ID: SV-269578r1054098
```

Rationale:

By default, the Xylok container is created not allowing users to modify any files inside the container.

The only paths that can be altered are mounted from the host. Mount the database files from the host, so that the database server running inside the container can write data.

If READONLY=false, then a user could go into the container as root and change other files. This approach helps protect the application from both external attacks and internal threats.

Audit:

Verify that Xylok's default read-only status is disabled by using the following command:

```
$ grep READONLY /etc/xylok.conf
```

If "READONLY" is set to False (case insensitive), is commented out or is missing, this is not a finding.

Remediation:

Revert Xylok to its default read-only configuration:

1. As root, open /etc/xylok.conf in a text editor.
2. Add/Amend "READONLY=True" to the configuration file.
3. Restart Xylok to apply settings:

```
systemctl restart xylok
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

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

1.10 XYLK-20-000053 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must disable nonessential capabilities.

```
GROUP ID: V-269579
RULE ID: SV-269579r1053512
```

Rationale:

If Xylok has unnecessary functionality enabled, the server may allow arbitrary code to run within the Xylok container. This would allow the user to potentially launch malicious acts against other hosts from inside the Xylok container.

ENABLE_PP_TEST_API setting in the Xylok Security Suite refers to a configuration flag that enables a specific test API related to the policy processing (PP) functionalities of the suite. This setting is used primarily in development or testing environments to enable specific testing functionalities.

Satisfies: SRG-APP-000141, SRG-APP-000246, SRG-APP-000247, SRG-APP-000384

Audit:

Verify that Xylok's default ENABLE_PP_TEST_API status is disabled by using the following command:

```
$ grep ENABLE_PP_TEST_API /etc/xylok.conf
```

If "ENABLE_PP_TEST_API" exists (case insensitive), this is a finding.

Remediation:

Revert Xylok to its default configuration, which disables the post-processing test API:

1. As root, open /etc/xylok.conf in a text editor.
2. Delete any ENABLE_PP_TEST_API lines from configuration file.
3. Restart Xylok to apply settings:

```
systemctl restart xylok
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

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

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)

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

1.11 XYLK-20-000109 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Xylok Security Suite configuration for DEBUG must be False.

```
GROUP ID: V-269580
RULE ID: SV-269580r1053515
```

Rationale:

Providing too much information in error messages risks compromising the data and security of the Xylok Security Suite and system. If DEBUG is set to True, it will show stack traces in error messages to assist with contact Xylok Support, but potentially reveal secure information.

Audit:

Verify DEBUG is configured. Execute the following:

```
$ grep DEBUG /etc/xylok.conf
```

DEBUG=False
If "DEBUG" is not set to False or is missing, this is a finding.

Remediation:

Set DEBUG:

1. As root, open /etc/xylok.conf in a text editor.
2. Add/Amend "DEBUG=False" to the configuration file.
3. Restart Xylok to apply settings by executing the following:

```
systemctl restart xylok
```

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

1.12 XYLK-20-000137 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must not allow local user or groups.

```
GROUP ID: V-269581
RULE ID: SV-269581r1054095
```

Rationale:

Active Directory’s (AD's) design to create but not delete local groups supports operational efficiency, system integrity, and compliance needs.

Manual checks will help identify user accounts that are no longer active or orphaned accounts which could pose security risks. Within Xylok there must not be a local users/groups. Manually verifying local users and groups ensures that unauthorized users do not gain access to sensitive resources.

Satisfies: SRG-APP-000328, SRG-APP-000715, SRG-APP-000720, SRG-APP-000725, SRG-APP-000730, SRG-APP-000735

Audit:

Verify the local accounts and groups are associated with AD and that user privileges are correct. Check accounts as a logged in administrator in Xylok.

1. Verify there are no local users. Navigate to User Menu >> Database Admin >> Users.
   If any local user(s) exist or users(s) are not current in AD, this is a finding.
   If any users have privileged access that do not require that access, this is a finding.
2. Verify there are no removed or local groups. Navigate to User Menu >> Database Admin >> Groups .
   Verify the only groups exist are created by AD and are currently being used by AD.
   If any groups exist that are not actively being used by AD, this is a finding.

Remediation:

Delete unused or local groups/users.

1. As a logged in administrator in Xylok, navigate to User Menu >> Database Admin >> Users.
2. Select User(s) to delete.
3. Click on down arrow in "Action".
4. Select "Delete selected users"
5. Click "Go".
6. Click "Yes, I'm sure".
7. Delete Group.
8. As a logged in administrator in Xylok, navigate to User Menu >> Database Admin >> Groups.
9. Select Group(s) to delete.
10. Click on down arrow in "Action".
11. Select "Delete selected users".
12. Click "Go".
13. Click "Yes, I'm sure".

Additional Information:

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

CCI-003638 Enforce organization-defined discretionary access control policies over defined subjects and objects where the policy specifies that a subject that has been granted access to information can pass the information to any other subjects or objects.

- NIST SP 800-53 Revision 5::AC-3 (4) (a)

CCI-003639 Enforce organization-defined discretionary access control policies over defined subjects and objects where the policy specifies that a subject that has been granted access to information can grant its privileges to other subjects.

- NIST SP 800-53 Revision 5::AC-3 (4) (b)

CCI-003640 Enforce organization-defined discretionary access control policies over defined subjects and objects where the policy specifies that a subject that has been granted access to information can change security attributes on subjects, objects, the system, or the system's components.

- NIST SP 800-53 Revision 5::AC-3 (4) (c)

CCI-003641 Enforce organization-defined discretionary access control policies over defined subjects and objects where the policy specifies that a subject that has been granted access to information can choose the security attributes to be associated with newly created or revised objects.

- NIST SP 800-53 Revision 5::AC-3 (4) (d)

CCI-003642 Enforce organization-defined discretionary access control policies over defined subjects and objects where the policy specifies that a subject that has been granted access to information can change the rules governing access control.

- NIST SP 800-53 Revision 5::AC-3 (4) (e)

1.13 XYLK-20-000161 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Xylok Security Suite configuration file must be protected.

```
GROUP ID: V-269582
RULE ID: SV-269582r1053521
```

Rationale:

Protecting the configuration file is a fundamental aspect of maintaining the security, integrity, and stability of Xylok Security Suite. By implementing robust protection mechanisms, Xylok can safeguard sensitive information, ensure compliance, and enhance operational reliability while minimizing the risks associated with unauthorized access and misconfigurations.

Audit:

Check the Xylok configuration file permissions with the following command:

```
$ ls -l /etc/xylok.conf
```

If this file has permissions greater than "0644", this is a finding.

Remediation:

As root, correct permissions for xylok.conf by running:

```
# chmod 0644 /etc/xylok.conf
```

Additional Information:

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

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

1.14 XYLK-20-000162 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must audit the enforcement actions used to restrict access associated with changes to it.

```
GROUP ID: V-269583
RULE ID: SV-269583r1053524
```

Rationale:

By default, auditing is not set up. Verifying that the host operating system generates audit records for events affecting /etc/xylok.conf is a critical security practice for Xylok. It enhances security monitoring, ensures accountability, supports compliance, maintains operational integrity, mitigates risks, and improves integration with security monitoring tools.

Without auditing the enforcement of access restrictions against changes to the Xylok Security Suite configuration, it will be difficult to identify attempted attacks and an audit trail will not be available for forensic investigation for after-the-fact actions.

Audit:

From the host machine as a normal user, verify the host OS generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/xylok.conf" with the following command:
Note: Directions are for Red Hat Enterprise Linux (RHEL) 8 and similar. If using a different OS, the steps may vary.

```
$ sudo grep /etc/xylok.conf /etc/audit/audit.rules
```

-w /etc/xylok.conf -p warx -k xylok_config
If the command does not return a line, or the line is commented out, this is a finding

Remediation:

Setting up auditing of a file in RHEL 8 involves using the auditd service and creating specific audit rules. Below are the steps to set up auditing for /etc/xylok.conf:

1. Ensure that the audit package is installed on your system by running the following:
   sudo dnf install audit
2. Start the auditd service if it is not already running:
   sudo systemctl start auditd
3. Enable the service to start automatically on boot:
   sudo systemctl enable auditd
4. Create an Audit Rule for the /etc/xylok.conf File:
   sudo auditctl -w /etc/xylok.conf -p warx -k xylok_config
5. Make the Audit Rule Persistent (optional):
   The rule set using auditctl will be active only until the next reboot. To make it persistent, add it to the /etc/audit/rules.d/audit.rules file.
   Open the file in a text editor:
   sudo vi /etc/audit/rules.d/audit.rules

Add the rule at the end of the file:
-w /etc/xylok.conf -p warx -k xylok_config

6. After making the rule persistent, restart the audit service to apply the changes:
   sudo systemctl restart auditd
7. The events related to the audited file will be recorded in /var/log/audit/audit.log. To view the logs, use the ausearch command:
   sudo ausearch -k xylok_config
8. To confirm that the rule is in place, list all current audit rules with:
   sudo auditctl -l

Additional Information:

CCI-003938 Automatically generate audit records of the enforcement actions.

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

1.15 XYLK-20-000191 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must only allow the use of DOD Public Key Infrastructure (PKI) established certificate authorities (CAs) for verification of the establishment of protected sessions.

```
GROUP ID: V-269584
RULE ID: SV-269584r1054096
```

Rationale:

Untrusted CAs can issue certificates, but they may be issued by organizations or individuals that seek to compromise DOD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DOD-approved CA, trust of this CA has not been established.

The DOD will only accept PKI certificates obtained from a DOD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of Transport Layer Security (TLS) certificates.

This requirement focuses on communications protection for the Xylok Security Suite session rather than for the network packet.

This requirement applies to applications that use communications sessions. This includes, but is not limited to, web-based applications and Service-Oriented Architectures (SOAs).

Audit:

Verify that the certificate Xylok uses for SSL is correctly signed with the following command. In this command, replace "xylok.local" with the domain named used to access the Xylok instance.

```
$ openssl s_client -showcerts -servername xylok.local -connect
xylok.local:443 </dev/null
```

CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = E5
verify return:1
depth=0 CN = xylok.local
verify return:1

Certificate chain
0 s:CN = xylok.local
i:C = US, O = Let's Encrypt, CN = E5
a:PKEY: id-ecPublicKey, 256 (bit); sigalg: ecdsa-with-SHA384
v:NotBefore: Jun 12 16:44:03 2024 GMT; NotAfter: Sep 10 16:44:02 2024 GMT
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
1 s:C = US, O = Let's Encrypt, CN = E5
i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
a:PKEY: id-ecPublicKey, 384 (bit); sigalg: RSA-SHA256
v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----

Server certificate
subject=CN = xylok.local
issuer=C = US, O = Let's Encrypt, CN = E5

No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits

SSL handshake has read 2367 bytes and written 380 bytes
Verification: OK

New, TLSv1.3, Cipher is TLS_AES_128_GCM_SHA256
Server public key is 256 bit
This TLS version forbids renegotiation.
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)

Post-Handshake New Session Ticket arrived:
SSL-Session:
Protocol : TLSv1.3
Cipher : TLS_AES_128_GCM_SHA256
Session-ID:
E03F9C6A59BD7375CF86B43387C63F9BBD16EAA2A9970E64F70E20317D403D22
Session-ID-ctx:
Resumption PSK:
15BFB16AF236A045FE9F5A0F64834A1B3EA76EE4185936D83560BAE940D01FF4
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 604800 (seconds)
TLS session ticket:
0000 - d4 7d 77 f4 01 dd ba 65-57 59 76 e0 ab 8a 75 63 .}w....eWYv...uc
0010 - 19 6e cf 1b 44 db 35 c5-27 6b d8 b8 39 76 10 47 .n..D.5.'k..9v.G
0020 - f1 75 a5 4b 3a fb 2b 82-b9 f7 3c c5 7f 82 41 d0 .u.K:.+...<...A.
0030 - 3d 40 f1 f4 0d ef 8e 55-ee 2f 09 4b 96 d9 16 5a =@.....U./.K...Z
0040 - f2 7d cb af bd 55 4b f9-c8 2d 0d 8f 39 16 af 8c .}...UK..-..9...
0050 - 71 df 92 cc d1 1a ed 5d-71 eb a3 7f f0 8b 65 8c q......]q.....e.
0060 - 5b 16 18 0c 61 b2 cc c7-4b [...a...K

```
Start Time: 1719438481
Timeout   : 7200 (sec)
Verify return code: 0 (ok)
Extended master secret: no
Max Early Data: 0
```

---

read R BLOCK
DONE
If the output indicates a "verify error", Xylok is using a self-signed certificate and this is a finding.
If the first certificate displayed is not a DOD-approved CA or other approved authority, this is a finding.

Remediation:

Generate or acquire certificates from DOD PKI (or other approved source).
Remove all files in /opt/xylok/certs.
Place new certificate in PEM format at /opt/xylok/certs/cert.crt.
Place new private key in PEM format at /opt/xylok/certs/key.key.
Restart Xylok:
systemctl restart xylok

Additional Information:

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

1.16 XYLK-20-000199 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Xylok Security Suite must maintain the confidentiality and disable the use of SMTP.

```
GROUP ID: V-269585
RULE ID: SV-269585r1053530
```

Rationale:

Disabling the use of SMTP within the Xylok Security Suite is a strategic decision aimed at enhancing security, ensuring compliance, and reducing operational risks. By eliminating the potential vulnerabilities associated with email communications, Xylok can better protect sensitive data and maintain a robust security posture.

Audit:

Verify USE_SMTP is configured by executing the following:

```
$ grep USE_SMTP /etc/xylok.conf
```

If "USE_SMTP" is not set to "False" or is missing, this is a finding.

Remediation:

Set USE_SMTP:

1. As root, open /etc/xylok.conf in a text editor.
2. Add/Amend "USE_SMTP=False" to the configuration file.
3. Restart Xylok to apply settings by executing the following:

systemctl restart xylok

Additional Information:

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

1.17 XYLK-20-000244 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must use a valid DOD-issued certification.

```
GROUP ID: V-269740
RULE ID: SV-269740r1054081
```

Rationale:

Without the use of a certificate validation process, the site is vulnerable to accepting certificates that have expired or have been revoked. This would allow unauthorized individuals access to the web server. This also defeats the purpose of the multi-factor authentication provided by the PKI process.

Audit:

Verify the Xylok Security Suite is using a valid DOD-issued certification with the following command:

```
$ openssl x509 -noout -text -in /opt/xylok/certs/cert.crt
```

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD Root CA 3
Validity
Not Before: Mar 20 18:46:41 2012 GMT
Not After : Dec 30 18:46:41 2029 GMT
Subject: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD Root CA 3
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
If the Issuer is not an approved authority, this is a finding.

Remediation:

1. Obtain DOD root certificate authority (CA)-signed certificate for the domain or generate a certificate using other approved provider.
2. Install the certificate in x509 format at /opt/xylok/certs/cert.crt
3. Restart Xylok: systemctl restart xylok

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.18 XYLK-20-000291 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Xylok Security Suite must use a central log server for auditing records.

```
GROUP ID: V-269586
RULE ID: SV-269586r1053533
```

Rationale:

Integrating a central log server for managing audit records within the Xylok Security Suite enhances security monitoring, incident response, and compliance efforts. By providing centralized logging, real-time analysis, and automated alerting, a central log server allows Xylok to maintain a robust security posture and effectively respond to potential threats, ultimately contributing to the organization's overall security strategy.

Satisfies: SRG-APP-000745, SRG-APP-000115, SRG-APP-000125, SRG-APP-000181, SRG-APP-000358, SRG-APP-000362, SRG-APP-000363, SRG-APP-000364, SRG-APP-000365, SRG-APP-000366, SRG-APP-000367, SRG-APP-000368, SRG-APP-000369, SRG-APP-000370, SRG-APP-000376, SRG-APP-000750, SRG-APP-000755, SRG-APP-000760, SRG-APP-000765, SRG-APP-000770, SRG-APP-000775, SRG-APP-000780, SRG-APP-000785, SRG-APP-000790, SRG-APP-000795, SRG-APP-000800, SRG-APP-000805, SRG-APP-000515

Audit:

Verify SIEM. On the host server, ensure /etc/rsyslog.d/101-xylok.conf exists and contains the following contents:
$ModLoad imfile
$InputFileName /var/log/xylok/api/current
$InputFileTag xylok-api:
$InputFileStateFile /tmp/xylok-api-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/db/current
$InputFileTag xylok-db:
$InputFileStateFile /tmp/xylok-db-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/mx/current
$InputFileTag xylok-mx:
$InputFileStateFile /tmp/xylok-mx-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/primary/current
$InputFileTag xylok-primary:
$InputFileStateFile /tmp/xylok-primary-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/web/current
$InputFileTag xylok-web:
$InputFileStateFile /tmp/xylok-web-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/worker/current
$InputFileTag xylok-worker:
$InputFileStateFile /tmp/xylok-worker-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
If the file contents do not monitor all logs in /var/log/xylok/, this is a finding.
If the rsyslog destination is not configured to send logs to a valid syslog server, this is a finding.
Note: The rsyslog destination host may appear in a different file, often following a format similar to “*. @siem.example.com:514.

Remediation:

Create /etc/rsyslog.d/100-xylok.conf with these contents, ensuring the final line points to a valid syslog server.

```
$ModLoad imfile
$InputFileName /var/log/xylok/api/current
$InputFileTag xylok-api:
$InputFileStateFile /tmp/xylok-api-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/db/current
$InputFileTag xylok-db:
$InputFileStateFile /tmp/xylok-db-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/mx/current
$InputFileTag xylok-mx:
$InputFileStateFile /tmp/xylok-mx-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/primary/current
$InputFileTag xylok-primary:
$InputFileStateFile /tmp/xylok-primary-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/web/current
$InputFileTag xylok-web:
$InputFileStateFile /tmp/xylok-web-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
$InputFileName /var/log/xylok/worker/current
$InputFileTag xylok-worker:
$InputFileStateFile /tmp/xylok-worker-log-state
$InputFileSeverity info
$InputFileFacility local3
$InputRunFileMonitor
```

Restart rsyslog to apply changes:

```
sudo systemctl restart rsyslog
```

Additional Information:

CCI-003821 Implement the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53 Revision 5::AU-6 (4)

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53::AU-7 (1)
- NIST SP 800-53A::AU-7 (1).1
- NIST SP 800-53 Revision 4::AU-7 (1)
- NIST SP 800-53 Revision 5::AU-7 (1)

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-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

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)

CCI-001875 Provide an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 4::AU-7 a

- NIST SP 800-53 Revision 5::AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001879 Provide a report generation capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001881 Provide an audit reduction capability that does not alter original content or time ordering of audit records.

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

CCI-001882 Provide a report generation capability that does not alter original content or time ordering of audit records.

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

CCI-001896 Enforce dual authorization for movement and/or deletion of organization-defined audit information.

- NIST SP 800-53 Revision 4::AU-9 (5)
- NIST SP 800-53 Revision 5::AU-9 (5)

CCI-003822 Implement an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 5::AU-7 a

CCI-003823 Implement an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 5::AU-7 a

CCI-003824 Implement an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 5::AU-7 a

CCI-003825 Implement a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 5::AU-7 a

CCI-003826 Implement a report generation capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 5::AU-7 a

CCI-003827 Implement a report generation capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 5::AU-7 a

CCI-003828 Implement an audit reduction capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 5::AU-7 b

CCI-003829 Implement a report generation capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 5::AU-7 b

CCI-003830 Implement the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53 Revision 5::AU-7 (1)

CCI-003831 Alert organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

- NIST SP 800-53 Revision 5::AU-9 b

CCI-003834 Implement the capability for organization-defined individuals or roles to change the auditing to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 5::AU-12 (3)

CCI-003938 Automatically generate audit records of the enforcement actions.

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

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)

1.19 XYLK-20-000334 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Xylok Security Suite must protect application-specific data.

```
GROUP ID: V-269569
RULE ID: SV-269569r1053482
```

Rationale:

The /var/lib/xylok directory is essential for storing various types of data necessary for the operation and functionality of the Xylok Security Suite. It acts as a central repository for application data, ensuring that the suite can function effectively and maintain state and configuration between sessions. Proper management and protection of this directory is crucial to ensure the security and stability of the application.

Audit:

Check the Xylok lib file permissions with the following command:

```
$ ls -l /var/lib/xylok
```

If "db" file has permissions greater than "0700", this is a finding.
If any other file or directory has permissions greater than "0755", this is a finding.

Remediation:

As root, correct permissions for xylok.conf by running:

```
# chmod -R 0755  /var/lib/xylok
# chmod -R 0700 /var/lib/xylok/data/db
```

Additional Information:

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	XYLK-20-000001 (Manual)	☐	☐
1.2	XYLK-20-000003 (Manual)	☐	☐
1.3	XYLK-20-000005 (Manual)	☐	☐
1.4	XYLK-20-000006 (Manual)	☐	☐
1.5	XYLK-20-000009 (Manual)	☐	☐
1.6	XYLK-20-000020 (Manual)	☐	☐
1.7	XYLK-20-000043 (Manual)	☐	☐
1.8	XYLK-20-000051 (Manual)	☐	☐
1.9	XYLK-20-000052 (Manual)	☐	☐
1.10	XYLK-20-000053 (Manual)	☐	☐
1.11	XYLK-20-000109 (Manual)	☐	☐
1.12	XYLK-20-000137 (Manual)	☐	☐
1.13	XYLK-20-000161 (Manual)	☐	☐
1.14	XYLK-20-000162 (Manual)	☐	☐
1.15	XYLK-20-000191 (Manual)	☐	☐
1.16	XYLK-20-000199 (Manual)	☐	☐
1.17	XYLK-20-000244 (Manual)	☐	☐
1.18	XYLK-20-000291 (Manual)	☐	☐
1.19	XYLK-20-000334 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 5, 2025	1.0.0	Initial CIS Release