



Keyboard, Video, and Mouse (KVM) Switch Checklist for SPAN STIG

Version 1, Release 1.3

19 December 2008

Developed by DISA for the DOD

UNCLASSIFIED

UNCLASSIFIED UNTILL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				

KVM01.001.00 V0006675 CAT III KVM Users Agreement

8500.2 IA Control: PRRB-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.1

Vulnerability Written user agreements for all users authorized to use the KVM or A/B switch are not being maintained..

Vulnerability Discussion A written users agreement allows the IAO to be certain the end user that will be using the equipment has been presented with the documentation that explains their duties and responsibilities in relation to the equipment and that they have acknowledged that they have read the documentation and understand it. Though there is no guarantee that user will perform as required, it will lessen the problems caused by uninformed users.
The IAO will maintain written user agreements for all users authorized to use the KVM or A/B switch.

Checks

SPAN KVM01.001.00

The reviewer will interview the IAO and view the written agreements.

The agreement will require the user to perform the following.

1. Logging onto an IS.
 - a. Identify the classification of the IS currently selected.
 - b. Use the login and passwords appropriate for that IS.
 - c. Verify the classification of the present IS by checking the classification label/banner.
 - d. Begin processing.
2. Switching between ISs.
 - a. Screen lock the IS you are currently working on if the IS supports this capability.
 - b. Select the desired IS with the switch.
 - c. Enter your user identifier and password to deactivate the screen lock on the newly selected IS.
 - d. Verify the classification of the present IS by checking the classification label/banner.
 - e. Begin processing.

The agreement may state that the user has read and understands the SFUG sections dealing with the KVM switch usage if the SFUG or similar documentation exists.

Default Finding Details Written user agreements for all users authorized to use the KVM or A/B switch are not being maintained..

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM01.001.00

Develop a user agreement, have each user of KVM or A/B switches sign a the user agreement, and keep the signed agreement on file.

Notes:

KVM01.002.00 V0006676 CAT III SFUG information for KVM and A/B switches.

8500.2 IA Control: PRRB-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.1

Vulnerability A SFUG, or an equivalent document, that describes the correct uses of the switch and the users responsibilities, is not being maintained and distributed.

Vulnerability Discussion The SFUG or an equivalent document describes the users security responsibilities including any site-specific requirements. This gives the user a single reference source for both initial indoctrination and for later review. The distribution of the SFUG will lessen the vulnerabilities create by user ignorance of policy or procedures required by the site. By keeping this document current the user will have the current policies and procedures available.
The IAO will maintain and distribute to the users a SFUG, or an equivalent document, that describes the correct uses of the switch and the users responsibilities.

Checks

SPAN KVM01.002.00

The reviewer will interview the IAO and review the documentation. SFUG is a Security Features User Guide. The SFUG will at a minimum have the following requirements.

1. Logging onto an IS.
 - a. Identify the classification of the IS currently selected.
 - b. Use the login and passwords appropriate for that IS.
 - c. Verify the classification of the present IS by checking the classification label/banner.
 - d. Begin processing.
2. Switching between ISs.
 - a. Screen lock the IS you are currently working on if the IS supports this capability.
 - b. Select the desired IS with the switch.
 - c. Enter your user identifier and password to deactivate the screen lock on the newly selected IS.
 - d. Verify the classification of the present IS by checking the classification label/banner.
 - e. Begin processing.

Default Finding Details A SFUG, or an equivalent document, that describes the correct uses of the switch and the users responsibilities, is not being maintained and distributed.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM01.002.00

If a Security Features User Guide does not exist, develop one making sure that there is a section for KVM and A/B switches containing the information found in the SPAN STIG.

If a Security Features User Guide exist create a section for KVM and A/B switches that contains the information found in the SPAN STIG.

Notes:

KVM01.003.00 V0006677 CAT I KVM switch physical security

8500.2 IA Control: PECF-1, PECF-2

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2

Vulnerability The KVM switch is not physically protected in accordance with the requirements of the highest classification for any IS connected to the KVM switch.

Vulnerability Discussion IF the KVM switch is not physically protected in accordance with the requirements of the highest classification for any IS connected to the KVM switch, the KVM switch can be tampered with leading to the compromise of sensitive data or a denial of service caused by the disruption of the systems the KVM switch is connected.
The IAO or SA will ensure that the KVM switch is physically protected in accordance with the requirements of the highest classification for any IS connected to the KVM switch.

Checks

SPAN KVM01.003.00

The reviewer will check the location of the KVM switch. Verify that it is located in area that is secured in the same manner as required of the IS with the highest classification level.

Default Finding Details The KVM switch is not physically protected in accordance with the requirements of the highest classification for any IS connected to the KVM switch.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM01.003.00

Develop a plan to move the KVM switch to a location that is physically protected in accordance with the requirements of the highest classification for any IS connected to the KVM switch. Obtain CM approval for the plan and implement the plan.

Notes:

KVM01.004.00 V0006678 CAT II KVM Smart (intelligent or programmable) keyboard

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2

Vulnerability Smart (intelligent or programmable) keyboard is used in conjunction with a KVM switch when the KVM switch is connected to ISs of different classification and/or sensitivity.

Vulnerability Discussion In an environment where the KVM switch is connected to ISs of different classification and/or sensitivity levels, a smart (intelligent or programmable) keyboard can transfer sensitive data from one system to another leading to the compromise of data. The IAO or SA will ensure that no smart (intelligent or programmable) keyboard is used in conjunction with a KVM switch when the switch is connected to ISs of different classification and/or sensitivity levels.

Checks

SPAN KVM01.004.00

The reviewer will interview the IAO and view the keyboard attached to verify that a smart keyboard is not in use when the KVM switch is attached to ISs with different clearance and/or sensitivity levels. Keyboards that include USB ports, smart card slots, and removable media slots are considered smart keyboards.

Note that a keyboard that has extended functionality that is not programmable, like an internet keyboard, is not prohibited.

Note: Having a CAC reader in the switch is acceptable, however, the host rather than the switch itself must perform the authentication algorithms. Otherwise the switch must be approved by PKI PMO.

Default Finding Details Smart (intelligent or programmable) keyboard is used in conjunction with a KVM switch when the switch is connected to ISs of different classification and/or sensitivity levels.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM01.004.00

Replace the smart keyboard with a keyboard that is not a smart keyboard.

Notes:

KVM01.005.00 V0006679 CAT II KVM Wireless keyboard and Mouse

8500.2 IA Control: ECWN-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2

Vulnerability A wireless keyboard or mouse that is not in compliance with the current Wireless STIG is attached to a KVM switch.

Vulnerability Signals from a wireless devices can be intercepted and decoded which can lead to the compromise of sensitive data.

Discussion The IAO or SA will ensure that wireless keyboards or mice attached to KVM switches are in compliance with the current Wireless STIG.

Checks

SPAN KVM01.005.00

The reviewer will look at the keyboard and the mouse. If either is wireless, verify that it is in compliance with the Wireless STIG section 2.4.

Default Finding A wireless keyboard or mouse that is not in compliance with the current Wireless STIG is attached to a KVM switch.

Details

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM01.005.00

Reconfigure the wireless device, if possible, to be compliant with the Wireless STIG section 2.4. If the wireless device cannot be made compliant with the Wireless STIG, replace the device with a wireless device that can be made compliant with the Wireless STIG or with a wire connected device.

Notes:

KVM01.006.00 V0006680 CAT III KVM Desktop Backgrounds

8500.2 IA Control: ECML-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2

Vulnerability The desktop backgrounds of ISs attached to a KVM switch are not labeled with banners in accordance with this STIG.

Vulnerability Discussion Without the banners to identify the IS that the KVM switch is currently active on, the user could enter a command to the wrong IS and create a denial of service or the user could enter data into the wrong system creating either a security incident (data entered to a system of the wrong classification) or a compromise of sensitive data.
The IAO or SA will ensure that the desktop backgrounds of ISs attached to a KVM switch are labeled with banners in accordance with this STIG.

Checks

SPAN KVM01.006.00

The reviewer will view the desktop backgrounds of the ISs attached to the KVM switch and verify that they are labeled as required.

The desktop backgrounds will display classification banners at the top and bottom of the screen.

These banners will state the overall classification level of the IS in large bold type.

These banners will have a solid background color assigned using the following scheme:

Yellow for Special Compartmented Information (SCI).

Orange for Top Secret (TS).

Red for Secret.

Blue for Confidential.

Green for Unclassified.

When ISs have similar classification levels but require separation for other reasons, the use of unique colors for different ISs or networks is permissible.

These banners will identify the IS if space is available

Default Finding Details The desktop backgrounds of ISs attached to a KVM switch are not labeled with banners in accordance with this STIG.

OPEN: NOT A FINDING: NOT REVIEWED: NOT APPLICABLE:

Fixes

SPAN KVM01.006.00

Modify the screen backgrounds for each IS attached to the KVM switch to comply with the guidance given in the STIG.

Notes:

KVM01.007.00 V0006681 CAT II KVM switch Configuration Password.

8500.2 IA Control: IAIA-1, IAIA-2

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3

Vulnerability The KVM switch has configurable features, but the configuration is not protected from modification with a DOD compliant password.

Vulnerability Discussion If the KVM switch is configurable, some feature that are available such as auto toggling between attached ISs are not permitted. If the configuration is not protected by a password it can be modified by any user allowing features that are not permitted. This can lead to the compromise of sensitive data.
If the KVM switch has configurable features, the IAO or SA will ensure that the configuration is protected from modification with a DOD compliant password.

Checks

SPAN KVM01.007.00

If the KVM switch is configurable, the reviewer will, with the assistance of the SA, try to change the configuration with a random password and with no password.

Note the emphasis here is the protection of the configuration not the technique, if the configuration is protected as a function of a privileged userid/password sign in to the KVM switch or by a DOD PKI (for network attached KVM switches) this fulfills this requirement.

Default Finding Details The KVM switch has configurable features, but the configuration is not protected from modification with a DOD compliant password.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM01.007.00

If the KVM switch's configuration can be protected by a password, including userid/password combinations or PKI for network attached switches, create a DOD compliant password to protect the configuration.

If the KVM switch's configuration cannot be protected by a password, including userid/password combinations or PKI for network attached switches, replace it with a KVM switch that either has no configuration or the configuration can be protected by a password.

Notes:

KVM01.008.00 V0006682 CAT II KVM Automatic Toggling between ISs

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3

Vulnerability The KVM switch has the feature for automatically toggling between ISs and it is not disabled.

Vulnerability Discussion The feature that automatically toggles between connected ISs or active ISs can cause a screen to be automatically displayed that contains sensitive information. This can lead to the compromise of sensitive data.
The IAO or SA will ensure that the feature for automatically toggling between ISs is disabled.

Checks

SPAN KVM01.008.00

If the KVM switch has the feature for automatically toggling between ISs, the reviewer will verify, with the assistance of the IAO or SA, that it is disabled. :If the feature is disable but the configuration is not protected then this is a finding.

Default Finding Details The KVM switch has the feature for automatically toggling between ISs and it is not disabled.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.008.00

Disable the feature for automatically toggling between ISs.
If the KVM switch can be configured to disable the ability to switch peripherals other than the keyboard, video monitor, and mouse, modify the configuration to disable this feature.
If the KVM switch cannot be configured to disable this feature replace the KVM switch with a KVM switch that is compliant with the SPAN STIG.

Notes:

KVM01.009.00 V0006683 CAT II KVM Miscellaneous hot key features

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3

Vulnerability A "hot key" feature is enabled other than the menu feature that allows the user to select the IS to be used from the displayed menu.

Vulnerability Discussion There are many "hot key" features that could be used. Since each vender has a different set of features and it is impractical to review all features for all vender for potential vulnerabilities, no features other than the ability to bring up a menu of the ISs available on the KVM switch to allow the user to select which IS they wish to display. Additional features will be approved if requested and time is available to review the feature and its implementation.
The IAO or SA will ensure that the only "hot key" feature enabled is the menu feature that allows the user to select the IS to be used from the displayed menu.

Checks

SPAN KVM01.009.00

The reviewer will, with the assistance of the IAO or SA, verify that the only "hot key" feature enabled is the menu feature that allows the user to select the IS to be used from the displayed menu. If the configuration cannot be protected this will be considered a finding.

Default Finding Details A "hot key" feature is enabled other than the menu feature that allows the user to select the IS to be used from the displayed menu.

OPEN: NOT A FINDING: NOT REVIEWED: NOT APPLICABLE:

Fixes

SPAN KVM01.009.00

Disable any unauthorized "hot key" features in the KVM switch's configuration.

Notes:

KVM01.011.00 V0006684 CAT III KVM Configuration Backup

8500.2 IA Control: COSW-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3

Vulnerability A machine-readable or a paper-document backup is not maintained for the configuration of the KVM switch.

Vulnerability Discussion Without a backup of the KVM switch's configuration, you can have a denial of service if the configuration cannot be restored quickly in the event that it is lost or a faulty switch needs to be replaced.
The IAO or SA will ensure that a machine-readable or a paper-document backup is maintained for the configuration of the KVM switch.

Checks

SPAN KVM01.011.00

Interview the IAO or SA to verify that a backup of the configuration is maintained.

Default Finding Details A machine-readable or a paper-document backup is not maintained for the configuration of the KVM switch.

OPEN: NOT A FINDING: NOT REVIEWED: NOT APPLICABLE:

Fixes

SPAN KVM01.011.00

Create a machine-readable or paper-document backup of the KVM switch configuration.

Notes:

KVM02.001.00 V0006685 CAT III KVM Physical description of connections

8500.2 IA Control: DCHW-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.1

Vulnerability A written description of the KVM switch, the ISs attached to the KVM switch, and the classification level of each IS attached to the KVM switch is not maintained.

Vulnerability Discussion Without a written description of the KVM switch, the ISs attached to the KVM switch, and the classification level of each IS attached to the KVM switch, tampering with the KVM switch by adding or moving connections cannot be verified and the physical configuration cannot be reproduced if needed. This can lead to a denial of service if a connection is removed or moved, or a compromise of sensitive data if a connection is added or moved.
The IAO will maintain a written description of the KVM switch, the ISs attached to the KVM switch, and the classification level of each IS attached to the KVM switch.

Checks

SPAN KVM02.001.00

The reviewer will verify that the description exists and check that it accurately describes the switch and its attached ISs. An annotated drawing or diagram is acceptable.

Default Finding Details A written description of the KVM switch, the ISs attached to the KVM switch, and the classification level of each IS attached to the KVM switch is not maintained.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.001.00

Create a written description of the KVM switch, the ISs attached to the KVM switch, and the classification level for each IS attached to the KVM switch.

Notes:

KVM02.002.00 V0006686 CAT II KVM Switch Configuration Password change

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.3

Vulnerability The KVM switch is not configured to force the change of the configuration password every 90 days or that there is no policy and procedure in place to change the configuration password every 90 days.

Vulnerability Discussion The longer time between password changes the greater the chance that the password will become compromised. A compromised password can allow a malicious user to change the configuration of the KVM switch creating a denial of service or a compromise of sensitive data.
The IAO will ensure that the KVM switch is configured to force the change of the configuration password every 90 days or that there is a policy and procedure in place to change the configuration password every 90 days.

Checks

SPAN KVM02.002.00

The reviewer will, with the assistance of the IAO or SA, verify that the KVM switch is configured to force the change of the configuration password every 90 days or that there is a policy and procedure in place to change the configuration password every 90 days.

Default Finding Details The KVM switch is not configured to force the change of the configuration password every 90 days or that there is no policy and procedure in place to change the configuration password every 90 days.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.002.00

Configure the KVM switch to force the change of the configuration password every 90 days or if the KVM switch does not support this functionality, create a policy and procedure to change the configuration password every 90 days.

Notes:

KVM02.003.00 V0006687 CAT I KVM switch RAS

8500.2 IA Control: EBRP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.3

Vulnerability The KVM switch has the ability to support a RAS connection, this feature is not disabled or the connectors on the KVM switch supporting this feature are not blocked with a tamper resistant seal.

Vulnerability Discussion KVM switches that support Dialup Remote Access (RAS) do not support a robust identification and authorization process or robust auditing. This feature will not be used. The tamper resistant seals over the port(s) that support this feature will serve as an indicator that the feature may have been used for unauthorized access to the KVM switch. The IAO has not ensured that if the KVM switch has the ability to support a RAS connection, this feature is disabled and the connectors on the KVM switch supporting this feature are blocked with a tamper resistant seal.

Checks

SPAN KVM02.003.00

The reviewer will, with the assistance of the IAO, will verify that if the KVM switch has the ability to support a RAS connection, this feature is disabled and the connectors on the KVM switch supporting this feature are blocked with a tamper resistant seal.

Default Finding Details The KVM switch has the ability to support a RAS connection, this feature is not disabled or the connectors on the KVM switch supporting this feature are not blocked with a tamper resistant seal.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.003.00

Configure the KVM switch to disable the RAS feature, remove all hardware from the KVM switch that supports this feature, and block all connectors on the KVM switch that support this feature with tamper resistant seals.

Notes:

KVM02.004.00 V0006698 CAT III DAA Written Permission KVM span classification

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.4

Vulnerability Written permission from the DAA responsible for each IS attached to a KVM switch that is attached to ISs of different classification levels is not being maintained.

Vulnerability Discussion The DAA responsible for a IS attached to a KVM switch that has other ISs attached of differing classifications levels must approve of the use of the KVM switch. The DAA is the only individual that may be cognizant of the nature of the data accessible from the IS and what requirements have been placed on its access. There may have a need to have the system isolated from KVM switches even though they are approved for use in spanning classification levels.
When the ISs are of different classification levels, the IAM will maintain written permission from all DAAs responsible for all ISs that are connected to a KVM switch.

Checks

SPAN KVM02.004.00

The reviewer will interview the IAM and verify that written permission from the DAA responsible for each IS attached to a KVM switch that is attached to ISs of different classification levels is being maintained. View the documentation.

Default Finding Details Written permission from the DAA responsible for each IS attached to a KVM switch that is attached to ISs of different classification levels is not being maintained.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.004.00

Obtain written permission for the IS to be attached to the KVM switch in accordance with the SPAN STIG from the DAA responsible for the system in question
At the earliest time so as not to impact production, if written permission has not received, the IS will be removed from the KVM switch and placed on a separate keyboard, video monitor, and mouse until written permission is received.

Notes:

KVM02.005.00 V0006699 CAT II KVM switch List for ISs differing classification

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.4

Vulnerability A KVM or A/B switch not found on an approved list or not installed using approved port configuration is connected to ISs that are at different classification levels.

Vulnerability Discussion Only KVM switches that have been tested and verified to prevent the transfer of data from one IS to another will be used when the ISs connected to the switch are of differing classification levels. The switch will be operated in the approved port configuration only. When the KVM switch is attached to ISs of different classification levels, the IAO will ensure that only approved KVM or A/B switches are used.

Checks

SPAN KVM02.005.00

The reviewer will verify that the KVM or A/B switch attached to ISs of different classification levels exists on one of the following lists.

1. The National Information Assurance Partnership (NIAP) National Information Assurance Certification and Accreditation Process (NIACAP) List.
2. DISN Security Accreditation Working Group (DSAWG) Approved KVM Switch List. The SIPRNet Connection Approval Office (SCAO) will maintain a DISN Approved Products List.

To locate the NIACAP list:

Go to <http://www.niap-ccivs.org/cc-scheme/vpl/> On the Validated Products page click on the column labeled "Technology" to sort by that column. Scroll down to entries with "Peripheral Switch" listed in the Technology column.

To Locate the DSAWG list:

Go to <https://powhatan.iiee.disa.mil/cap/documentation/index.html#siprnet>. This information is located under the document titled DISN Peripheral Sharing Device Guidance. Refer to the power point file of the document to locate the list.

Default Finding Details A KVM or A/B switch that is not found on an approved list is connected to ISs that are at different classification levels.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.005.00

Immediately replace the unapproved KVM switch with an approved KVM switch. If there is not an approved KVM switch available, remove all ISs from the unapproved KVM switch and attach a separate keyboard, video monitor, and mouse to each IS. Alternately the ISs can be segregated by classification level on as many KVM switches, that are compliant with the SPAN STIG, as needed. Verify port configuration complies with guidance for the switch used.

Notes:

KVM02.006.00 V0006700 CAT III KVM Differing Classification levels Cascaded

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.4

Vulnerability A KVM switch is cascaded while being attached to ISs of different classification levels.

Vulnerability Discussion Cascading KVM switches, connecting one switch to another switch, can make it difficult to determine which system is currently connected to the keyboard, video and mouse by simple observation. In situations where the ISs are of differing classification levels this could lead to the compromise of sensitive or classified data or a denial of service caused by a privileged command being given to the wrong system.
When the KVM switch is attached to ISs of different classification levels, the IAO or SA will ensure that no KVM switches are cascaded.

Checks

SPAN KVM02.006.00

The reviewer will check the connections for the KVM switch to verify that it is not connected to another KVM switch when ISs of different classification levels are attached.

Default Finding Details A KVM switch is cascaded while being attached to ISs of different classification levels.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.006.00

Develop a plan to remove all cascaded KVM switches as soon as possible without disrupting production. Connect each IS to an open port on a KVM switch that is in turn only connected to a keyboard, video monitor, and mouse, not to another KVM switch. Obtain CM approval for the plan and execute the plan at the earliest opportunity.

Notes:

KVM02.007.00 V0006701 CAT II KVM Spanning Classification Level Tamper Seals

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.4

Vulnerability Tamper resistant seals are not attached to the KVM switch and all IS cables at their attachment points where the KVM switch is attached to ISs of different classification levels.

Vulnerability Discussion Tamper resistant seals are tape designed to break if tampered with. They are used to indicate that a cabinet has been opened or a cable removed, moved or added. For KVM switches attached to ISs of differing classification levels it is necessary to be aware of any potential tampering with the connections. Switching the cables for two ISs could lead to the compromise of sensitive data. Removal of a cable could lead to a denial of service until it is reattached.
The IAO or SA will ensure that tamper resistant seals are attached to the KVM switch and all IS cables at their attachment points.

Checks

SPAN KVM02.007.00

The reviewer will verify that tamper resistant seals are attached to the KVM switches and to the IS cable attachment points. For cables these seals will be place across the junction between the switch and the cable. For the KVM witch the seals will be placed across the KVM case joints so that opening the case will break the seal.

Default Finding Details Tamper resistant seals are not attached to the KVM switch and all IS cables at their attachment points where the KVM switch is attached to ISs of different classification levels.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.007.00

Obtain tamper resistant seals and apply them to the KVM switch case joints so that if the case is open the seal will be broken. Also place them across the junction between the IS cables and the KVM switch so that if a cable is moved or removed the seal will be broken.

Notes:

KVM02.008.00 V0006702 CAT I KVM Differing Classification Switch Peripheral

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.4

Vulnerability A KVM switch is being used to switch a peripheral other than a keyboard, video or mouse in an environment where the KVM switch is attached to ISs of different classification levels..

Vulnerability Discussion Since the other peripheral devices could contain persistent memory and allow data to become compromised by moving it between ISs of differing classification levels this would create an unacceptable situation. This includes the ability to switch a smart card reader. If the switch has this ability and it is not disabled it will be assumed that it is being used.
When the KVM switch is attached to ISs of different classification levels, the IAO or SA will ensure, if the KVM switch has the ability to switch peripheral devices other than the keyboard, video, and mouse, that this feature is disabled.

Checks

SPAN KVM02.008.00

The reviewer will, with the assistance of the IAO or SA, verify that the KVM switch is not configured to switch peripherals other than a Keyboard, Video, and Mouse.

Note: This includes but is not limited to a smart card reader.

Note: The most likely interface that would be used with this feature would be USB but it may be any legacy I/O interfaces.

Default Finding Details A KVM switch is being used to switch a peripheral other than a keyboard, video or mouse in an environment where the KVM switch is attached to ISs of different classification levels..

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.008.00

Disable the feature for automatically toggling between ISs.
If the KVM switch can be configured to disable the ability to switch peripherals other than the keyboard, video monitor, and mouse, modify the configuration to disable this feature.
If the KVM switch cannot be configured to disable this feature replace the KVM switch with a KVM switch that is compliant with the SPAN STIG.

Notes:

KVM02.009.00 V0006703 CAT I KVM Differing Classification Peripherals Attached

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.4

Vulnerability Peripherals other than a keyboard, video, or mouse are attached to a KVM switch that is attached to ISs of different classification levels.

Vulnerability Discussion It will be assumed that any peripheral other than a keyboard, video monitor, or mouse attached to a KVM switch is intended to be used regardless of the current configuration of the KVM switch. This peripheral can contain persistent memory that can be used to move data between ISs of different classification levels compromising either the data that was moved and the IS to which the data was moved. When the KVM switch is attached to ISs of different classification levels, the IAO, the SA, and the user will ensure that no peripheral other than the keyboard, video, or mouse is connected to the KVM.

Checks

SPAN KVM02.009.00

The reviewer will view the KVM switch, used in an environment where it is attached to ISs of different clearance levels, to verify that no peripherals other than the keyboard, video, and mouse are attached.

Default Finding Details Peripherals other than a keyboard, video, or mouse are attached to a KVM switch that is attached to ISs of different classification levels.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.009.00

Remove the unauthorized peripheral and block the ports it is attached to with tamper resistant seals.

Notes:

KVM02.010.00 V0006704 CAT II KVM Differing Classification Unblocked Ports

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.4

Vulnerability A KVM switch, which is attached to ISs of different classification levels, has connectors for additional peripherals other than the keyboard, video, or mouse that are not blocked with tamper resistant seals.

Vulnerability Discussion It will be assumed that KVM switches that can switch peripherals other than the keyboard, video monitor, and mouse, that are attached to ISs of differing classification levels, and that do not have the connectors for the additional peripherals blocked with tamper resistant seals, have been tampered with and have been used to transfer data between ISs of different classifications levels until proven otherwise. If data is transferred between ISs of different classification levels the data has been compromised and the receiving IS has been compromised.
When the KVM switch is attached to ISs of different classification levels, the IAO or SA will ensure that the connectors for additional peripherals are blocked with tamper resistant seals.

Checks

SPAN KVM02.011.00

The reviewer will view the KVM switch, which is attached to ISs of different classification levels, to verify that all connectors for peripherals other than a keyboard, video or mouse are blocked with tamper resistant seals.

Default Finding A KVM switch, which is attached to ISs of different classification levels, has connectors for additional peripherals other than the keyboard, video, or mouse that are not blocked with tamper resistant seals.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM02.011.00

Obtain tamper resistant seals and apply them across the connectors for peripherals other than the keyboard, video monitor, and mouse on KVM so the if a cable is attached to the connector the seal will be broken.

Notes:

KVM03.001.00 V0006705 CAT I Network KVM used to Administer not Out-of-Band

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3

Vulnerability A network attached KVM switch used to administer ISs is not attached to an "out-of-band" network.

Vulnerability Discussion If a network attached KVM switch is attached to an out-of-band network there is less opportunity for a malicious user to compromise the interface and create a denial of service by issuing disruptive commands to a server.
The IAO or SA will ensure a network attached KVM switch used to administer ISs is connected to an "out-of-band" network.

Checks

SPAN KVM03.001.00

The reviewer will interview the IAO or SA to verify that a network attached KVM switch used to administer ISs is connected to an "out of band" network.

Default Finding Details A network attached KVM switch used to administer ISs is not attached to an "out-of-band" network.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.001.00

Develop a plan that will attach all network attached KVM switches used to administer ISs to a out-of-band network. Obtain CM approval and implement the plan.

Notes:

KVM03.002.00 V0006706 CAT I Network KVM Classification of Network

8500.2 IA Control: ECIC-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3

Vulnerability The network attached KVM switch is attached to a network that is not at the same classification level as the ISs attached.

Vulnerability Discussion If a network attached KVM switch is attached to a network of a different classification level than the ISs attached to the KVM switch, this will lead to a compromise of sensitive data either on the network or on the ISs.
The IAO will ensure that network attached KVM switches are only connected to a network that is at the same classification level as the ISs attached

Checks

SPAN KVM03.002.00

The reviewer will interview the IAO to verify that a network attached KVM switch is attached to a network of the same classification level as the ISs attached.

Default Finding Details The network attached KVM switch is attached to a network that is not at the same classification level as the ISs attached.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.002.00

Remove the KVM switch from the network when the KVM IS attached to the KVM switch are at a different classification level then the network. Attach the KVM switch to a network of the appropriate classification level.

Notes:

KVM03.003.00 V0006707 CAT I Network KVM Network Infrastructure Compliance

8500.2 IA Control: DCCS-1, DCCS-2

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.2

Vulnerability The network-facing component of a network attached KVM switch is not compliant with the current Network Infrastructure STIG.

Vulnerability Discussion If the network facing components of a network attached KVM switch are not in compliance with the Network Infrastructure STIG the KVM switch could expose the network to vulnerabilities that could lead to a denial of service caused by the disruption of the network or a compromise of sensitive data.

Checks

SPAN KVM03.003.00

The reviewer will interview the IAO to verify that a Network review has been performed on the network that the KVM switch is attached and that all findings discovered during the network review dealing with the KVM switch have been closed.

Default Finding Details The network-facing component of a network attached KVM switch is not compliant with the current Network Infrastructure STIG.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.003.00

Perform a self-assessment on the network the KVM switch is attached or request FSO to schedule and perform a Network review. Following the review close all findings.

Notes:

KVM03.004.00 V0006708 CAT I Network KVM Login

8500.2 IA Control: IAIA-1, IAIA-2

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.3

Vulnerability The KVM switch is not configured to require the user to login to the KVM switch to access the ISs attached.

Vulnerability Discussion Without identification and authentication of the user accessing the network attached KVM switch anyone can access the ISs attached and if they have knowledge of a valid userid and password for the IS disrupt the system causing a denial of service or access sensitive data compromising that data.
The IAO will ensure that the KVM switch is configured to require the user to login to the KVM switch to access the ISs attached. PKI authentication is acceptable and preferred to password authentication.

Checks

SPAN KVM03.004.00

The reviewer will, with the assistance of the IAO, try to access the network attached KVM switch without valid authentication

Default Finding Details The KVM switch is not configured to require the user to login to the KVM switch to access the ISs attached.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.004.00

Reconfigure the network attached KVM switch to require the users to login to the KVM switch prior to being allowed access to the ISs attached to the KVM switch.

Notes:

KVM03.005.00 V0006709 CAT I Network KVM DOD Complaint Password

8500.2 IA Control: IAIA-1, IAIA-2

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.3

Vulnerability The KVM switch is not configured to require DOD compliant password.

Vulnerability Strong passwords are harder to guess or discover via brut force making the system more secure from malicious tampering.

Discussion The IAO will ensure that the KVM switch is configured to require DOD compliant password.

Checks

SPAN KVM03.005.00

The reviewer will, with the assistance of the IAO, try to change a password to a non-compliant password. The use of PKI authentication would make this a check not a finding.

Default Finding The KVM switch is not configured to require DOD compliant password.

Details

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.005.00

Reconfigure the network attached KVM switch to require DOD compliant Passwords. If this is not possible replace the KVM switch with a KVM switch that can be configured to enforce DOD compliant passwords.

Notes:

KVM03.006.00 V0006710 CAT I Network KVM Group Userid

8500.2 IA Control: IAGA-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.3

Vulnerability Group or shared userids are being used on a network attached KVM switch.

Vulnerability Usage of group or shared userids makes it impossible to attribute an action to the originating user. In the case of a malicious action this could make prosecution impossible.

Discussion The IAO will ensure that group or shared userids are not used.

Checks

SPAN KVM03.006.00

The reviewer will interview the IAO verify that a group or shared userids are not being used.

Default Finding Group or shared userids are being used on a network attached KVM switch.

Details

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.006.00

Remove the shared or group userid and issue individual userids to each user who requires access to the network attached KVM switch.

Notes:

KVM03.007.00 V0006711 CAT III Network KVM Users Restricted to ISs.

8500.2 IA Control: ECAN-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.3

Vulnerability The network attached KVM switch is not configured to restrict users access only to the systems they require.

Vulnerability Users accessing ISs that they do not access to can lead to the compromise of sensitive data.

Discussion The IAO will ensure that the KVM switch is configured to restrict users access only to the systems they require.

Checks

SPAN KVM03.007.00

The reviewer will, with the assistance of the IAO, try to access a system not allowed to the user signed onto the network attached KVM switch.

Default Finding The network attached KVM switch is not configured to restrict users access only to the systems they require.

Details

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.007.00

Reconfigure the network attached KVM switch to restrict users to systems they need to access.

Notes:

KVM03.008.00 V0006712 CAT III Network KVM Warning Banner

8500.2 IA Control: ECWM-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM)
6510.01, "Defense-in-Depth: Information Assuran ,
SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.3

Vulnerability The network attached KVM switch does not display an Electronic Notice and Consent Banner complaint with requirements of CJSCM 6510.01.

Vulnerability The warning banner notifies the user that they are accessing a DOD system and that they consent to having their actions monitored.

Discussion Without this banner it is difficult to prosecute individuals who violate the usage restrictions of the IS.

Checks

SPAN KVM03.008.00

The reviewer will, with the assistance of the IAO or the SA, access the network attached KVM switch to verify that a compliant warning banner is displayed.

Default Finding The network attached KVM switch does not display an Electronic Notice and Consent Banner complaint with requirements of CJSCM

Details 6510.01.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.008.00

Reconfigure to network KVM switch to display a warning banner in accordance with the SPAN STIG.

Notes:

KVM03.009.00 V0006713 CAT I Network KVM Encryption

8500.2 IA Control: ECNK-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.3

Vulnerability The KVM switch is not configured to use encrypted communications with FIPS 140-1/2 validated cryptography.

Vulnerability Discussion Because all administrative traffic contains sensitive data such as unencrypted passwords, it will be encrypted to protect it from interception. The KVM switch will be configured to require encryption for all communications via the network. NIST FIPS 140-1/2 validated cryptography will be used. The IAO or SA will ensure that the KVM switch is configured to use encrypted communications using FIPS 140-1/2 validated cryptography.

Checks

SPAN KVM03.009.00

The reviewer will, with the assistance of the IAO or SA, verify that the network attached KVM switch is configured for encryption using FIPS 140-1/2 validated cryptography.

Default Finding Details The KVM switch is not configured to use encrypted communications with FIPS 140-1/2 validated cryptography.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.009.00

Reconfigure the network KVM switch to use FIPS-140-1/2 validated cryptography for all communications across the network.

Notes:

KVM03.010.00 V0006714 CAT I Network Encapsulated USB non KVM Traffic

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.3

Vulnerability The KVM switch is configured to encapsulate and send USB connections other than KVM connections.

Vulnerability Discussion Some network attached KVM switched can encapsulate USB connections other than the keyboard, video monitor, and mouse connections. This connection could be a disk drive connection and could allow the transfer of data between the ISs attached to the KVM switch and the client system attached via IP to the KVM switch leading to a compromise of sensitive data. The IAO or SA will ensure that the KVM switch is not configured to encapsulate and send USB connections other than KVM connections.

Checks

SPAN KVM03.010.00

The reviewer will, with the assistance of the IAO or SA, verify that the KVM switch is not configured to encapsulate and send USB connections other than KVM connections.

Default Finding Details The KVM switch is configured to encapsulate and send USB connections other than KVM connections.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.010.00

Reconfigure the network KVM switch so that it will not encapsulate USB connections other than the keyboard, video monitor, or mouse, over IP.

Notes:

KVM03.011.00 V0006715 CAT II Network KVM Unused USB Ports Tamper Seals

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.3

Vulnerability Unused USB ports on the KVM switch are not blocked with tamper resistant on a KVM switch that can encapsulate and send the USB protocol over the network to the client.

Vulnerability Discussion By blocking the unused USB ports on the network attached KVM switch that can encapsulate USB over IP with tamper resistant seals we will have an indication if someone has attached an unauthorized USB connection to the KVM switch. When a broke seal if found it should be investigated.
The IAO will ensure that the USB ports on the KVM switch are blocked with tamper resistant seals if no USB connections are made to a KVM switch that can encapsulate and send the USB protocol over the network to the client

Checks

SPAN KVM03.011.00

if the KVM switch can encrypt USB and send it over the network, the reviewer will view the KVM switch and verify that unused USB ports are blocked with tamper resistant seals.

Default Finding Details Unused USB ports on the KVM switch are not blocked with tamper resistant on a KVM switch that can encapsulate and send the USB protocol over the network to the client.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.011.00

Block unused USB ports on a network attached KVM switch that can encapsulate USB over IP with tamper resistant seals.

Notes:

KVM03.012.00 V0006716 CAT II Network KVM Power Control of IS

8500.2 IA Control: DCBP-1, PECF-1, PECF-2

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.3

Vulnerability A network attached KVM switch is configured to control the power supplied to the ISs attached to the KVM switch or the connectors on the KVM switch that support this feature are not blocked with tamper resistant seals.

Vulnerability Discussion If a network attached KVM switch can control the power to the ISs attached to it and the KVM switch is compromised, a denial of service can be caused by powering off all the ISs attached to the KVM switch without accessing the individual ISs.
The IAO will ensure that any feature that allows the KVM switch to directly control the power supplied to the ISs is not configured or used, and that any connectors on the KVM switch used to support this feature are blocked with a tamper resistant seal.

Checks

SPAN KVM03.012.00

wWith the assistance of the IAO, verify that the network attached KVM switch is not configured to control the power of the ISs attached and that all connectors on the KVM switch that support this functionality are blocked with tamper resistant seals.

Default Finding Details A network attached KVM switch is configured to control the power supplied to the ISs attached to the KVM switch or the connectors on the KVM switch that support this feature are not blocked with tamper resistant seals.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.012.00

Remove the KVM switch's control over the power supplied to the ISs and block any connectors on the KVM switch used to support this feature with a tamper resistant seals.

Notes:

KVM03.013.00 V0006717 CAT I Network KVM ISs of different Classification Levels

8500.2 IA Control: ECIC-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.4

Vulnerability A network attached KVM switch is attached to ISs of different classification levels.

Vulnerability Discussion Because of the problems inherent in the spanning of networks of different classification levels, network attached KVM switches will not be attached to ISs of different classification levels. This can lead to the compromise of sensitive data.
The IAO will ensure the network attached KVM switches are not attached to ISs of different classification levels.

Checks

SPAN KVM03.013.00

The reviewer will interview the IAO to verify that a network attached KVM switch is not attached to ISs of different classification levels.

Default Finding Details A network attached KVM switch is attached to ISs of different classification levels.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM03.013.00

Remove all ISs from the network attached KVM switch that have a classification level that is different from the classification level of the network the KVM switch is attached to. Use a new network attached KVM switch for each classification level that you have ISs which were removed from the original KVM switch. Attach the KVM switch to a network that has the same classification level as the ISs that has been attached to the KVM switch.

Notes:

KVM04.001.00 V0006718 CAT III A/B Switch User Agreements

8500.2 IA Control: PRRB-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.1

Vulnerability There are no user agreements documenting the use of A/B switches.

Vulnerability Discussion A signed users agreement is proof that the user has been informed of his security responsibilities when using an A/B switch.
The IAO will maintain written user agreements for all users authorized to use an A/B switch.

Checks

SPAN KVM04.001.00

The reviewer will interview the IAO and view the user agreements. A signed addendum to the SAAR is acceptable.

Default Finding Details There are no user agreements documenting the use of A/B switches.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.001.00

Create a standard user agreement for the use of A/B switches and have all authorized users of A/B switches sign them.

Notes:

KVM04.002.00 V0006719 CAT III A/B switch SFUG

8500.2 IA Control: PRRB-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.1

Vulnerability There is no user documentation describing the correct usage and users responsibilities for an A/B switch.

Vulnerability Discussion The Security Features Users Guide (SFUG) gives the users a single source to find security policy and guidance as to the users responsibility for security. The general policies and user responsibilities as apply to A/B switches and any local security policies will be placed in the SFUG or similar document.
The IAO will maintain and distribute to the users a SFUG that describes the correct uses of the switch and the users responsibilities.

Checks

SPAN KVM04.002.00

The reviewer will interview the IAO and view the SFUG or equivalent documentation to verify that the following points are discussed.

1. A/B switches should be used only if there is no other solution.
2. A/B switches should be used only to connect multiple peripheral devices to a single IS.
3. A/B switches should never be used to connect a single peripheral to multiple ISs.
4. If an A/B switch is used to connect or share peripheral devices between two or more ISs, the ISs should be intended for the use of a single user within the users work area, and be visible from all ISs that it is attached.

Default Finding Details There is no user documentation describing the correct usage and users responsibilities for an A/B switch.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.002.00

Create a section in the sites SFUG that contains general security policies and guidance plus the site security policies and guidance for use of an A/B switch.

Notes:

KVM04.003.00 V0006720 CAT I A/B Switch Physical protection

8500.2 IA Control: PECF-1, PECF-2

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.2

Vulnerability The A/B switch is not physically protected in accordance with the requirements of the highest classification of any IS connected to the A/B switch.

Vulnerability Discussion If the A/B switch is not located in an area that has the same physical security as required by the IS of the highest clearance level this can lead to a compromise of sensitive data.
The IAO or SA will ensure that the A/B switch is physically protected in accordance with the requirements of the highest classification for any IS connected to the A/B switch.

Checks

SPAN KVM04.003.00

The reviewer will view the A/B switch to verify that it is physically protected in accordance with the requirements of the highest classification of any IS connected to the A/B switch. If it is in the same location as the ISs connected then it is adequately protected.

Default Finding Details The A/B switch is not physically protected in accordance with the requirements of the highest classification of any IS connected to the A/B switch.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.003.00

Move the A/B switch to a location where it is protected in the same manner as required by the IS of the highest clearance level the A/B switch is attached.

Notes:

KVM04.004.00 V0006757 CAT II A/B Switch Sharing Peripheral Between Users

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.2

Vulnerability An A/B switch is used to share a peripheral device between two or more users.

Vulnerability Discussion When using a KVM switch to switch a peripheral between two or more users the risk always exists where the peripheral is connected to the wrong IS. An example would be a scanner where the user presses a button on the scanner which causes the IS the scanner is currently to initiate a scan. If the A/B is pointed to a different IS than the user intended the document would be scanned into the wrong system. This could lead to the compromise of sensitive data.
The IAO or SA will ensure that an A/B switch is not used to share a peripheral device between two or more users.

Checks

SPAN KVM04.004.00

The reviewer will interview the IAO or SA to verify that A/B switches are not being used to share peripherals between two users.

Default Finding Details An A/B switch is used to share a peripheral device between two or more users.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.004.00

Develop a plan to remove all A/B switches that are being used to switch peripherals between two or more users and to acquire new peripherals to support documented needs. Obtain CM approval of the plan and execute the plan.

Notes:

KVM04.005.00 V0006758 CAT III A/B Switch Marking and Labeling

8500.2 IA Control: ECML-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.2

Vulnerability The A/B switch is not marked in accordance with the Sharing Peripherals Across the Network STIG.

Vulnerability Discussion Failure to correctly mark switch positions and cable connections can lead to the A/B switch connecting the wrong device to the wrong system for the current intended use. This can lead to a denial of access to a peripheral by an IS or the access of the wrong peripheral by an IS compromising sensitive data.
The IAO or SA will ensure that the A/B switch, cables, switch positions, and connectors are labeled in accordance with this STIG.

Checks

SPAN KVM04.005.00

The reviewer will view the A/B switch to verify that it is marked in accordance with the STIG. It is marked government owned equipment. The switch positions are marked as to the systems or peripherals connected. The cables and connectors are marked with the systems or peripherals that are connected and their clearance level.

Default Finding Details The A/B switch is not marked in accordance with the Sharing Peripherals Across the Network STIG.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.005.00

Mark and Label the A/B switches in accordance with the SPAN STIG.

Notes:

KVM04.006.00 V0006759 CAT II A/B switch on ISs of Different Classification

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.4

Vulnerability An A/B switches are used with ISs of differing classification levels that are not on the approved lists.

Vulnerability Discussion An A/B switch not found on the Approved KVM and A/B Switch lists has not been tested to verify that it does not leak data between systems. This can lead to the compromise of sensitive data or the compromise of the ISs attached to the A/B switch. The IAO will ensure that only approved KVM or A/B switches are used with ISs of differing classification levels.

Checks

SPAN KVM04.006.00

The reviewer will verify that the KVM or A/B switch attached to ISs of different classification levels exists on one of the following lists.

1. The National Information Assurance Partnership (NIAP) National Information Assurance Certification and Accreditation Process (NIACAP) List.
2. DISN Security Accreditation Working Group (DSAWG) Approved KVM Switch List. The SIPRNet Connection Approval Office (SCAO) will maintain a DISN Approved Products List.

To locate the NIACAP list:

Go to <http://niap.nist.gov> and follow the link to "Validated Products" found in the left most column of the screen. On the Validated Products page follow the link to "Peripheral Switch" found in the bottom row second column of the table.

To Locate the DSAWG list.

Go to <https://iase.disa.mil/cap>. This information is located under the document titled DISN Peripheral Sharing Device Guidance. Refer to the power point file of the document to locate the list.

Default Finding An A/B switches are used with ISs of differing classification levels that are not on the approved lists.

Details

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.006.00

Replace the A/B switch with one from the approved KVM and A/B switch lists. If there is no A/B switch on the lists that performs the function needed, remove the A/B switch and obtain whatever hardware is need to restore the functionality required.

Notes:

KVM04.007.00 V0006760 CAT II A/B Different Classification Tamper Seals

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.4

Vulnerability Tamper resistant seals are not attached to the A/B switch and all IS cables at their attachment points for A/B switches attached to devices or ISs that have different classification levels.

Vulnerability Discussion Without the presences of tamper resistance seals the A/B switch or its connections can be tampered with and the tampering will go undetected. This can lead to the compromise of sensitive data or the compromise of an IS. When an A/B switch is attached to ISs of different clearance levels the IAO or SA will ensure that tamper resistant seals are attached to the A/B switch and all IS cables at their attachment points.

Checks

SPAN KVM04.007.00

The reviewer will, for an A/B switch attached to devices or ISs which are at different classification levels, view the A/B switch to verify that tamper resistant seals are attached to the A/B switch and all IS cables at their attachment points.

Default Finding Details Tamper resistant seals are not attached to the A/B switch and all IS cables at their attachment points for A/B switches attached to devices or ISs that have different classification levels.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.007.00

For an A/B switch attached to devices or ISs which are at different classification levels, attached tamper resistant seals as required by the SPAN STIG.

Notes:

KVM04.008.00 V0006761 CAT III A/B Cascaded Differing Classification

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.4

Vulnerability A/B switches, that are connected to devices or ISs which are at different classification levels, are cascaded.

Vulnerability Discussion When A/B switches are cascaded it is difficult to verify that the currently selected connection is the correct selection. When A/B switches are used with ISs of differing classification levels this can lead to the compromise of sensitive data. When A/B switches are attached to ISs of different classification levels the IAO or SA will ensure that A/B switches are not cascaded.

Checks

SPAN KVM04.008.00

The reviewer will, for A/B switches, which are connected to devices or ISs that are at different classification levels, view the A/B switch to verify that A/B switches are not cascaded.

Default Finding Details A/B switches, that are connected to devices or ISs which are at different classification levels, are cascaded.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.008.00

Remove the cascaded A/B switches that are connected to ISs of different classification levels.

Notes:

KVM04.009.00 V0006762 CAT I A/B Switch Different Classification Disk

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.4

Vulnerability The An A/B switch is used to switch a peripheral device that has persistent memory or devices that support removable media between two or more ISs of different classification levels.

Vulnerability Discussion If the peripheral device attached to an A/B switch, which is connected to ISs of differing classification levels, can be written to and read from this can lead to the compromise of sensitive or classified data and/or the compromise of the ISs.
The IAO or SA will ensure that A/B switches are not used to switch a peripheral device that has persistent memory or devices that support removable media between two or more ISs of different classification levels.

Checks

SPAN KVM04.009.00

The reviewer will view the A/B switch to verify that the A/B switch is not used to switch a peripheral device that has persistent memory or devices that support removable media between two or more ISs of different classification levels. This would include but not be limited to ZIP drives, hard disk drives, and writable CD drives.

Default Finding Details The An A/B switch is used to switch a peripheral device that has persistent memory or devices that support removable media between two or more ISs of different classification levels.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.009.00

Remove the A/B switch used to switch a peripheral device that has persistent memory or devices that support removable media between two or more ISs of different classification levels.

Notes:

KVM04.010.00 V0006763 CAT I A/B I/O Peripherals Different Classification

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK
SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.4

Vulnerability Input or output devices including, but not limited to, scanners, printers or plotters are attached to an A/B switches that spans classification levels.

Vulnerability Discussion Input devices attached to A/B switches that are in turn attached to ISs of different classification levels could input data to the wrong IS compromising sensitive or classified data and/or the IS involved.
Output from output devices attached to A/B switches that are in turn attached to ISs of different classification levels could be picked up by an individual other than the one the data was intended, leading to a compromise of sensitive or classified data.
The IAO will ensure input and output devices including but not limited to scanners, printers or plotters are not attached to A/B switches that span classification levels.

Checks

SPAN KVM04.010.00

The reviewer will view the A/B switch to verify that input and output devices including, but not limited to, scanners, printers or plotters are not attached to an A/B switch that spans classification levels.

Default Finding Details Input or output devices including, but not limited to, scanners, printers or plotters are attached to an A/B switches that spans classification levels.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

SPAN KVM04.010.00

Remove the A/B switch that is attached to an input or output peripheral and the A/B switch is connected to ISs of different classification levels.

Notes: