UNCLASSIFIED

Multifunction Device and Network Printers STIG

Version: 2

Release: 4

24 Oct 2014

XSL Release 6/19/2012 Sort by: STIGID
Description:

Group ID (Vulid): V-6777
Group Title: MFD Protocol TCP/IP
Rule ID: SV-6999r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD01.001
Rule Title: A network protocol other than TCP/IP is enabled on a MFD or printer.

Vulnerability Discussion: The greater the number of protocols allowed active on the network the more vulnerabilities there will be available to be exploited. The SA will ensure the only network protocol used is TCP/IP all others are disabled.

Responsibility: System Administrator
IAControls: DCPP-1

Check Content:
The reviewer will, with the assistance of the SA, verify that the only network protocol enabled is TCP/IP.

Fix Text: Disable all protocols in the MFD except TCP/IP.

Group ID (Vulid): V-6778
Group Title: MFD or a printer is not using a static IP address
Rule ID: SV-7000r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD01.002
Rule Title: A MFD or a printer is not using a static IP address.

Vulnerability Discussion: Without static IP addresses, if the DNS cache is poisoned (corrupted) print files containing sensitive data could be redirected, leading to the compromise of sensitive data.

The SA will ensure all MFDs and printers are assigned a static IP.

Responsibility: System Administrator
IAControls: DCBP-1

Check Content:
The reviewer will, with the assistance of the SA, verify that the MFD or printer is assigned a static IP address.

Fix Text: Reconfigure the MFD or printer, assigning it a static IP address. One acceptable method could also be implemented using DHCP. The printer may be configured to obtain an IP address from DHCP, however, the IP reservation must be configured such that the address cannot ever be assigned to another device.

Group ID (Vulid): V-6779
Group Title: MFD/Printer Firewall/Router Rule Perimeter
Rule ID: SV-7001r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD01.003
Rule Title: A firewall or router rule is not used to block all ingress and egress traffic from the enclave perimeter to the MFD or printer.

Vulnerability Discussion: Access to the MFD or printer from outside the enclave network could lead to a denial of service caused by a large number of large print files being sent to the device. Ability for the MFD or printer to access addresses outside the enclave network could lead to a compromise of sensitive data caused by forwarding a print file to a location outside of the enclave network. This is good defence in depth practice.
The SA will ensure there is a firewall or router rule to block all ingress and egress traffic from the enclave perimeter to the MFD or printer.

Responsibility: System Administrator
IAControls: DCBP-1

Check Content:
The reviewer will interview the SA to verify that there is a firewall or router rule to block all ingress and egress traffic from the enclave perimeter to the MFD or printer.

Fix Text: Ensure that there is a firewall or router rule to block all ingress and egress traffic from the enclave perimeter to the MFD or printer.

Group ID (Vulid): V-6781
Group Title: MFD SNMP Community Strings
Rule ID: SV-7003r1_rule
Severity: CAT I
Rule Version (STIG-ID): MFD02.001
Rule Title: The default passwords and SNMP community strings of all management services have not been replaced with complex passwords.

Vulnerability Discussion: There are many known vulnerabilities in the SNMP protocol and if the default community strings and passwords are not modified a unauthorized individual could gain control of the MFD or printer. This could lead to a denial of service or the compromise of sensitive data.
The SA will ensure the default passwords and SNMP community strings of all management services are replaced with complex passwords.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
The reviewer will, with assistance from SA, verify that the default passwords and SNMP community strings of all management services have not been replaced with complex passwords.

Fix Text: Develop a plan to coordinate the modification of the default passwords and SNMP community strings of all management services replacing them with complex passwords. Obtain CM approval of the plan and execute the plan.

Group ID (Vulid): V-6782
Group Title: MFD Configuration State After Power Down or Reboot
Rule ID: SV-7004r1_rule
Severity: CAT I
Rule Version (STIG-ID): MFD02.002
Rule Title: The MFD does not maintain its configuration state (passwords, service settings etc) after a power down or reboot.

Vulnerability Discussion: If the MFD does not maintain it state over a power down or reboot, it will expose the network to all of the vulnerabilities that where mitigated by the modifications made to its configuration state.
The SA will ensure the MFD maintains its configuration state (passwords, service settings etc) after a power down or reboot.

Responsibility: System Administrator
IAControls: DCSS-1, DCSS-2

Check Content:
Interview the SA and review the MFD documentation to verify that the MFD will maintain its configuration state (passwords, service settings etc) after a power down or reboot.

Fix Text: Replace the MFD with a MFD that will maintain its configuration state (passwords, service settings etc) after a power down or reboot.

Group ID (Vulid): V-6783
Group Title: MFD Management Protocols
Rule ID: SV-7005r2_rule
Severity: CAT II
Rule Version (STIG-ID): MFD02.003
Rule Title: Management protocols, with the exception of HTTPS and SNMPv3, must be disabled at all times except when necessary.

Vulnerability Discussion: Unneeded protocols expose the device and the network to unnecessary vulnerabilities.

Responsibility: System Administrator
IAControls: DCPP-1

Check Content:
Verify that all management protocols are disabled unless approved by the organization's AO/ISSM.

Protocols may be enabled temporarily if needed to upgrade firmware or configure the device, but must be disabled immediately when this activity is completed. HTTPS and SNMPv3 may be used but must be configured in accordance with the requirements of the Network Infrastructure STIG.

If management protocols other than HTTPS and SNMPv3 are enabled unnecessarily or without AO/ISSM approval, this is a finding.

Fix Text: Disable all management protocols except HTTPS and SNMPv3 unless approval has been granted by the organization's AO/ISSM.

Group ID (Vulid): V-6780
Group Title: MFD Firmware
Rule ID: SV-7002r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD02.004
Rule Title: A MFD or a printer device is not flash upgradeable or is not configured to use the most current firmware available.

Vulnerability Discussion: MFD devices or printers utilizing old firmware can expose the network to known vulnerabilities leading to a denial of service or a compromise of sensitive data.
The SA will ensure devices are flash upgradeable and are configured to use the most current firmware available

Potential Impacts:
Upgrading the firmware may require taking the device offline making it unavailable while the process is being completed. Additionally, on some devices, if the process of updating the firmware is interrupted, the device may be disabled and unable to be upgraded or enabled without the manufactures representative intervening.

Responsibility: System Administrator
IAControls: VIVM-1

Check Content:
The reviewer will, with the assistance of the SA, verify that the devices are flash upgradeable and are configured to use the most current firmware available.

Fix Text: If the MFD or printer cannot be upgraded replace it.

If the MFD or printer can be upgraded but is not using the latest release of the firmware, upgrade the firmware.

Group ID (Vulid): V-6784

Group Title: MFD or a printer can be managed from any IP
Rule ID: SV-7009r1_rule
Severity: CAT I
Rule Version (STIG-ID): MFD02.005
Rule Title: There is no restriction on where a MFD or a printer can be remotely managed.

Vulnerability Discussion: Since unrestricted access to the MFD or printer for management is not required the restricting the management interface to specific IP addresses decreases the exposure of the system to malicious actions. If the MFD or printer is compromised it could lead to a denial of service or a compromise of sensitive data.
The SA will ensure devices can only be remotely managed by SA's or printer administrators from specific IPs (SA workstations and print spooler).

Responsibility: System Administrator
IAControls: DCBP-1

Check Content:
The reviewer will, with the assistance of the SA, verify that the MFD or printer can only be remotely managed by SA or printer administrator from specific IPs (SA workstations and print spooler). Look for list that restricts the protocol used for administrative access to specific IP addresses.

Fix Text: Restrict access to the MFD's or printer's management function to a specific set of IP addresses. If the device lacks this functionality use an ACL in a router, firewall or switch to restrict the access.

Group ID (Vulid): V-6790
Group Title: Print Services Restricted to Port 9100 and/or LPD
Rule ID: SV-7015r1_rule
Severity: CAT III
Rule Version (STIG-ID): MFD03.001
Rule Title: Print services for a MFD or printer are not restricted to Port 9100 and/or LPD (Port 515). Where both Windows and non-Windows clients need services from the same device, both Port 9100 and LPD can be enabled simultaneously.

Vulnerability Discussion: Printer services running on ports other than the known ports for printing cannot be monitored on the network and could lead to a denial of service it the invalid port is blocked by a network administrator responding to an alert from the IDS for traffic on an unauthorized port.

Potential Impacts:
Print clients configured to use the unauthorized port(s) will not be able to print until they are reconfigured to use the correct port.

Responsibility: System Administrator
IAControls: DCBP-1

Check Content:
The reviewer will, with the assistance of the SA, verify that the MFD or printer print services are restricted to LPD or port 9100.

Where both Windows and non-Windows clients need services from the same device, both Port 9100 and LPD can be enabled simultaneously.

Fix Text: Develop a plan to coordinate the reconfiguration of the printer servers and clients so that print services runs only on authorized ports. Obtain CM approval of the plan and implement the plan.

Group ID (Vulid): V-6794
Group Title: MFD/Printer Restrict Jobs Only From Print Spooler
Rule ID: SV-7019r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD04.001
Rule Title: A MFD or a printer is not configured to restrict jobs to those from print spoolers.

Vulnerability Discussion: If MFDs or printers are not restricted to only accepting print jobs from print spoolers that authenticate the user and log the job, a denial of service can be created by the MFD or printer accepting one or more large print jobs from an unauthorized user.
The SA will ensure MFDs and printers are configured to restrict jobs to only print spoolers, not directly from users.

The configuration is accomplished by restricting access, by IP, to those of the print spooler and SAs. If supported, IP restriction is accomplished on the device, or if not supported, by placing the device behind a firewall, switch or router with an appropriate discretionary access control list.

Potential Impacts:
Client systems that are configured to bypass the print server that spools the print will lose access the printer until reconfigured.

Responsibility: System Administrator

IAControls: DCBP-1

Check Content:
The reviewer will, with the assistance of the SA, verify that MFDs and printers are configured to restrict jobs to only print spoolers, not directly from users.

The configuration is accomplished by restricting access, by IP, to those of the print spoolers and SAs. If supported, IP restriction is accomplished on the device or if not supported, by placing the device behind a firewall, switch or router with an appropriate discretionary access control list.

Fix Text: Reconfigure the device to restrict access, by IP, to those of the print spoolers and SAs. If the device does not support this functionality, place the device behind a firewall, switch or router with an appropriate discretionary access control list.

Group ID (Vulid): V-6796
Group Title: MFD Authorized Users Restrictions
Rule ID: SV-7021r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD05.001
Rule Title: Print spoolers are not configured to restrict access to authorized users and restrict users to managing their own individual jobs.

Vulnerability Discussion: If unauthorized users are allowed access to the print spooler they can queue large print file creating a denial of service for other users. If users are not restricted to manipulating only files they created, they could create ad denial of service by changing the print order of existing files or deleting other users files.
The SA will ensure print spoolers are configured to restrict access to authorized user and restrict users to managing their own individual jobs.

Responsibility: System Administrator
IAControls: ECAN-1, IAIA-1, IAIA-2

Check Content:
The reviewer will, with the assistance of the SA, verify that the print spoolers are configured to restrict access to authorized users and restrict users to managing their own individual jobs.

Fix Text: Configure the print spoolers to restrict access to authorized users and restrict users to managing their own individual jobs.

Group ID (Vulid): V-6797
Group Title: MFD and Spooler Auditing
Rule ID: SV-7022r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD06.001
Rule Title: The devices and their spoolers do not have auditing enabled.

Vulnerability Discussion: Without auditing the identification and prosecution of an individual that performs malicious actions is difficult if not impossible.

Responsibility: System Administrator
IAControls: ECAR-1, ECAR-2, ECAR-3

Check Content:
The reviewer will, with the assistance of the SA, verify that devices and their spoolers have auditing fully enabled.

Fix Text: Configure the devices and their spoolers have auditing fully enabled.

Group ID (Vulid): V-6798
Group Title: MFD/Printer Security Policy
Rule ID: SV-7023r1_rule
Severity: CAT III
Rule Version (STIG-ID): MFD06.002
Rule Title: There is no security policy containing the requirements found in the SPAN STIG. Acceptable use of device storage and retransmission of data (DODD 5200.1-R, Appendix G) Verification that devices are not being shared on networks of different classification levels. Procedures for scrubbing or disposing of hard disks when devices are sent out for repair or disposal. Defined protocols for the maintenance, disposal, and purging of classified devices to include their non-volatile memory and storage devices. Defined protocols for acceptable key operator codes, administration passwords, user codes, which personnel can change them, how often, format and storage of codes, and passwords.

Vulnerability Discussion: These policies are designed to raise the overall awareness of security practices and procedures. Failure to follow them can lead to the compromise of sensitive data.

The IAO will ensure implementation of a MFD and printer security policy to include:

Acceptable use of device storage and retransmission of data (DODD 5200.1-R, Appendix G)
Verification that devices are not being shared on networks of different classification levels.
Procedures for scrubbing or disposing of hard disks when devices are sent out for repair or disposal.
Defined protocols for the maintenance, disposal, and purging of classified devices to include their non-volatile memory and storage devices.
Defined protocols for acceptable key operator codes, administration passwords, user codes, which personnel can change them, how often, format and storage of codes, and passwords.

Responsibility: Information Assurance Officer
IAControls: DCBP-1, ECAN-1, ECIC-1, IAIA-1, IAIA-2, PECS-1, PECS-2, PEDD-1

Check Content:
Interview the IAO to verify that there is a security policy that meets the requirements of the SPAN STIG implemented.

Fix Text: Implement a MFD and printer security policy in accordance with the SPAN STIG.

Group ID (Vulid): V-6799
Group Title: MFD Level of Audit and Reviewing
Rule ID: SV-7024r1_rule
Severity: CAT III
Rule Version (STIG-ID): MFD06.006
Rule Title: The level of audit has not been established by the IAO or the audits logs being collected for the devices and print spoolers are not being reviewed.

Vulnerability Discussion: If inadequate information is captured in the audit, the identification and prosecution of malicious user will be very difficult. If the audits are not regularly reviewed suspicious activity may go undetected for a long time.
The IAO will define a level of auditing to perform to include who reviews the audit logs.

Responsibility: Information Assurance Officer
IAControls: ECAR-1, ECAR-2, ECAR-3, ECAT-1, ECAT-2

Check Content:
The reviewer will interview the IAO to verify that the level of auditing has been established and that audit logs are being reviewed.

Auditing will include user, key operator and admin codes and passwords, enabled features and services. Any deviation from the baseline should be treated as a potential security incident. Ensure operational security controls are in place to ensure servicing of devices by authorized personnel is in accordance with change and configuration protocols.

Fix Text: Implement a level of auditing in accordance with the requirements in the SPAN STIG and establish a procedure to ensure regular review or the audit logs.

Group ID (Vulid): V-6800
Group Title: MFD Classified Network
Rule ID: SV-7025r2_rule
Severity: CAT I
Rule Version (STIG-ID): MFD07.001
Rule Title: MFDs with print, copy, scan, or fax capabilities must be prohibited on classified networks without the approval of the DAA.

Vulnerability Discussion: MFDs with print, copy, scan, or fax capabilities, if compromised, could lead to the compromise of classified data or the compromise of the network. The IAO will ensure MFDs with copy, scan, or fax capabilities are not allowed on classified networks unless approved by the DAA.

Potential Impacts:
If the device is removed from the classified network it will need to be sanitized in accordance with DoDD 5200.1R if it is to be used for unclassified processing or is to be decommissioned.

Responsibility: Information Assurance Officer
IAControls: DCBP-1

Check Content:
The reviewer will interview the IAO to verify that MFDs with print, copy, scan, or fax capabilities are prohibited on classified networks unless approved by the

DAA.

Fix Text: Remove the MFD from the classified network until DAA approval is obtained.

Group ID (Vulid): V-6801
Group Title: MFD Clearing Disk Space Scan to Disk
Rule ID: SV-7026r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD07.002
Rule Title: A MFD device, with scan to hard disk functionality used, is not configured to clear the hard disk between jobs.

Vulnerability Discussion: If the MFD is compromised the un-cleared, previously used, space on the hard disk drive can be read which can lead to a compromise of sensitive data.
The SA will ensure the device is configured to clear the hard disk between jobs if scan to hard disk functionality is used.

Responsibility: System Administrator
IAControls: ECRC-1

Check Content:
The reviewer, with the assistance of the SA, verify the device is configured to clear the hard disk between jobs if scan to hard disk functionality is used.

Note: This policy is a security-in-depth measure and applies to normal use. Thus, the clearing algorithm does not have to comply with DoD sanitization procedures. Proper sanitization using a DoD compliant procedure will be required only for final destruction/disposition.

Note: This does not apply if PKI authenticated access and discretionary access controls (authorization controls) are used to protect the stored data.

Fix Text: Configured the MFD to clear the hard disk between jobs if scan to hard disk functionality is used.

Group ID (Vulid): V-6802
Group Title: MFD Scan Discretionary Access Control
Rule ID: SV-7027r1_rule
Severity: CAT III
Rule Version (STIG-ID): MFD07.003
Rule Title: Scan to a file share is enabled but the file shares do not have the appropriate discretionary access control list in place.

Vulnerability Discussion: Without appropriate discretionary access controls unauthorized individuals may read the scanned data. This can lead to a compromise of sensitive data.
The SA will ensure file shares have the appropriate discretionary access control list in place if scan to a file share is enabled.

Responsibility: System Administrator
IAControls: ECAN-1

Check Content:
The reviewer will, with the assistance of the SA, verify that file shares have the appropriate discretionary access control list in place if scan to a file share is enabled.

Fix Text: Create the appropriate discretionary access control list for file shares if scan to a file share is enabled.

Group ID (Vulid): V-6803
Group Title: MFD Fax from Network Auditing
Rule ID: SV-7028r1_rule
Severity: CAT III
Rule Version (STIG-ID): MFD07.004
Rule Title: Fax from the network is enabled but auditing of user access and fax log is not enabled.

Vulnerability Discussion: Without auditing the originator and destination of a fax cannot be determined. Prosecuting of an individual who maliciously compromises sensitive data via a fax will be hindered without audits.
The SA will ensure auditing of user access and fax log is enabled if fax from the network is enabled.

Responsibility: System Administrator

IAControls: ECAR-1, ECAR-2, ECAR-3

Check Content:
The reviewer will, with the assistance of the SA, verify that auditing of user access and fax log is enabled if fax from the network is enabled.

Fix Text: Configure the MFD to audit faxing in accordance with the SPAN STIG. If this is not possible, disable the fax functionality and disconnect the phone

line from the MFD.

Group ID (Vulid): V-6804
Group Title: MFD Scan to SMTP (email)
Rule ID: SV-7029r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD07.005
Rule Title: Devices allow scan to SMTP (email).

Vulnerability Discussion: The SMTP engines found on the MFDs reviewed when writing the SPAN STIG did not have robust enough security features supporting scan to email. Because of the lack of robust security scan to email will be disabled on MFD devices. Failure to disable this feature could lead to an untraceable and possibly undetectable compromise of sensitive data.
The SA will ensure devices do not allow scan to SMTP.

Responsibility: System Administrator
IAControls: DCBP-1

Check Content:
The reviewer will, with the assistance of the SA, verify that devices do not allow scan to SMTP.

Note: With DAA approval, strict usage policies, and user training, MFD scan to SMTP (email) is allowed if CAC/PKI authentication is implemented on the MFD. There must be a method implemented for non-repudiation and authenticated access. A USB/flash drive/thumb drive or any removable storage capability will not be installed.

Fix Text: Disable the scan to SMTP (email) feature on all MFDs.

Group ID (Vulid): V-6805
Group Title: MFD Hard Drive Lock
Rule ID: SV-7030r1_rule
Severity: CAT II
Rule Version (STIG-ID): MFD08.001
Rule Title: A MFD device does not have a mechanism to lock and prevent access to the hard drive.

Vulnerability Discussion: If the hard disk drive of a MFD can be removed from the MFD the data on the drive can be recovered and read. This can lead to a compromise of sensitive data.

The IAO will ensure the device has a mechanism to lock and prevent access to the hard disk.

Responsibility: Information Assurance Officer
IAControls: PECF-1, PECF-2

Check Content:
The reviewer will, with the assistance of the SA, verify that the device has a mechanism to lock and prevent access to the hard disk.

What we are looking for here is a locking mechanism with a key securing the hard drive or the case access to the hard drive. The lock will be locked or this is a finding.

Note: This is not required if physical security measures are in place, if the drive is not easily removable, if drive is encrypted, or if there is zeroization or other strong protection mechanism.

Fix Text: If the lock is not locked, lock it.

If there is no lock see if the vendor makes one and if so acquire it an lock the drive.
If the vendor does not supply a lock, acquire an aftermarket lock that will secure the drive so that it cannot be accessed. Even a drive that cannot be removed but the connectors can be removed is vulnerable.

Group ID (Vulid): V-6806
Group Title: MFD/Printer Global Configuration Settings
Rule ID: SV-7031r1_rule
Severity: CAT I
Rule Version (STIG-ID): MFD08.002
Rule Title: The device is not configured to prevent non-printer administrators from altering the global configuration of the device.

Vulnerability Discussion: If unauthorized users can alter the global configuration of the MFD they can remove all security. This can lead to the compromise of sensitive data or the compromise of the network the MFD is attached to.

Responsibility: System Administrator
IAControls: ECAN-1

Check Content:
The reviewer will, with the assistance of the SA, verify that the device is configured to prevent non-printer administrators from altering the global configuration of the device.

Fix Text: Configured the device to prevent non-printer administrators from altering the global configuration of the device. If the device cannot be configured in this manner, replace the device with one that can be configured in an acceptable manner.

UNCLASSIFIED