Threat Modeling Report

Created on 11/7/2018 8:39:55 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

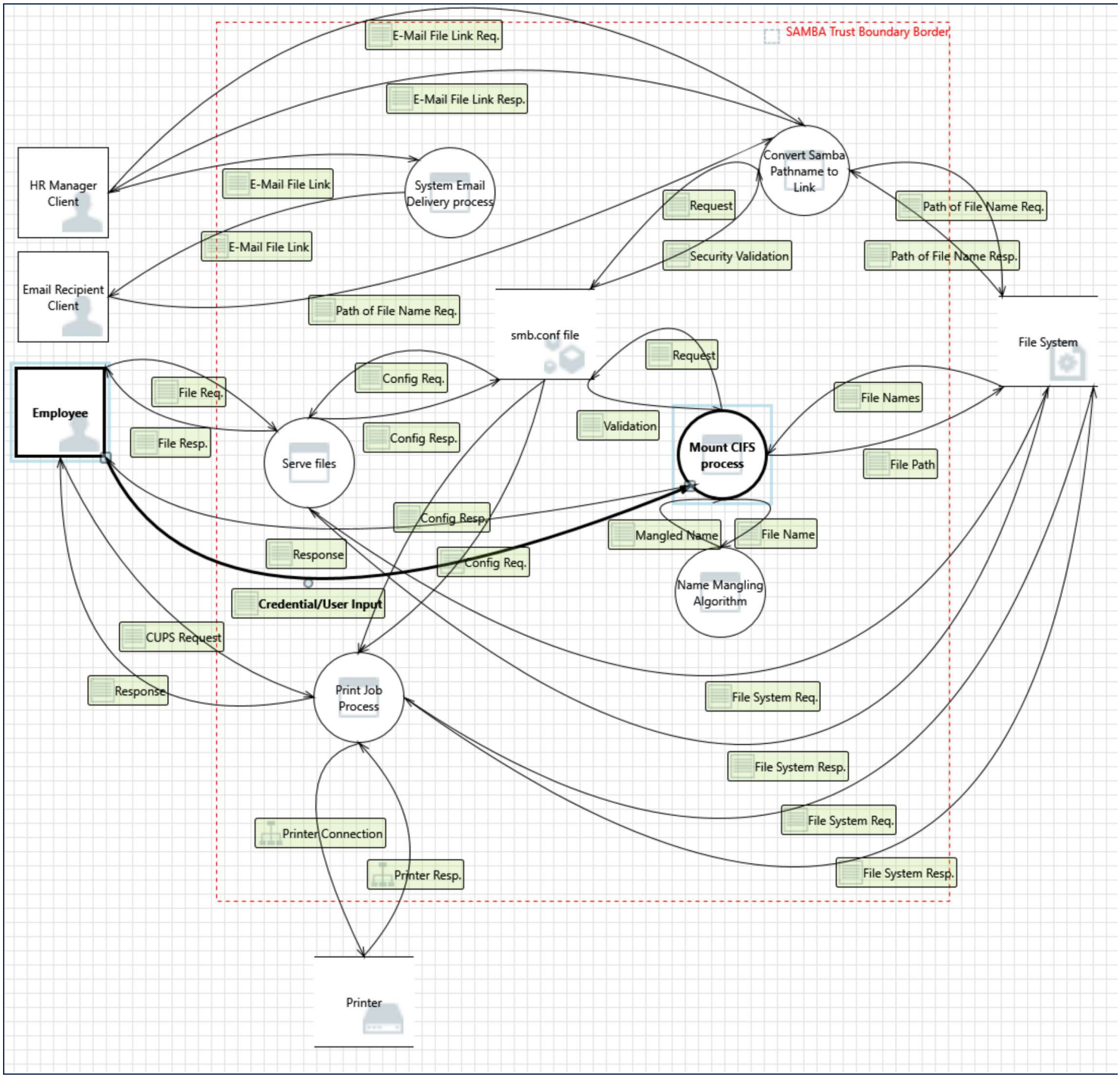
Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	11
Needs Investigation	0
Mitigation Implemented	167
Total	178
Total Migrated	0

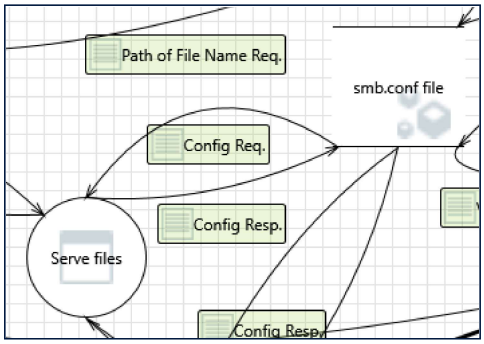
Diagram: Samba



Samba Diagram Summary:

Not Started	0
Not Applicable	11
Needs Investigation	0
Mitigation Implemented	167
Total	178
Total Migrated	0

Interaction: Config Req.



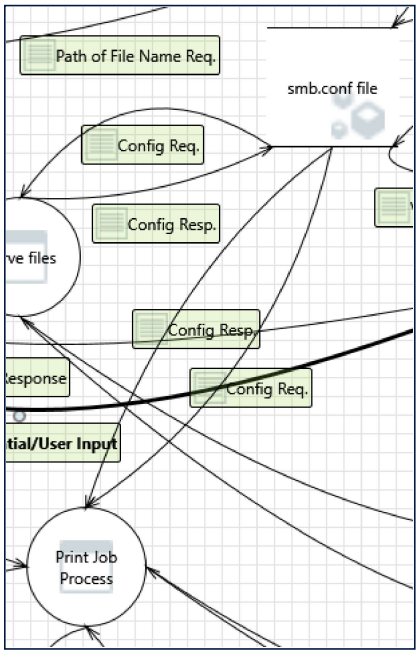
1. Spoofing of Source Data Store smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: smb.conf file may be spoofed by an attacker and this may lead to incorrect data delivered to Serve files. Consider using a standard authentication mechanism to identify the source data store.
Justification: Smb.conf can only be in etc/Samba and only root can edit etc/

2. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of smb.conf file can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: SMB packets are encrypted

Interaction: Config Req.



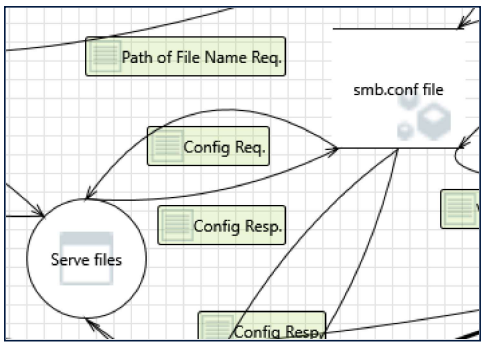
3. Spoofing of Source Data Store smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: smb.conf file may be spoofed by an attacker and this may lead to incorrect data delivered to Print Job Process. Consider using a standard authentication mechanism to identify the source data store.
Justification: Smb.conf can only be in etc/Samba and only root can edit etc/

4. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of smb.conf file can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: SMB packets are encrypted

Interaction: Config Resp.



5. Spoofing of Destination Data Store smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: smb.conf file may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of smb.conf file. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Smb.conf can only be in etc/Samba and only root can edit etc/

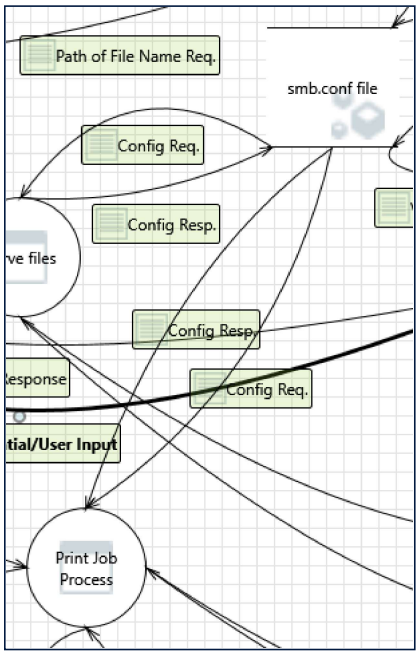
6. Potential Excessive Resource Consumption for Serve files or smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Serve files or smb.conf file take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Samba operates according to the OS resource controls

Interaction: Config Resp.



7. Spoofing of Source Data Store smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: smb.conf file may be spoofed by an attacker and this may lead to incorrect data delivered to Print Job Process. Consider using a standard authentication mechanism to identify the source data store.

Justification: Smb.conf can only be in etc/Samba and only root can edit etc/

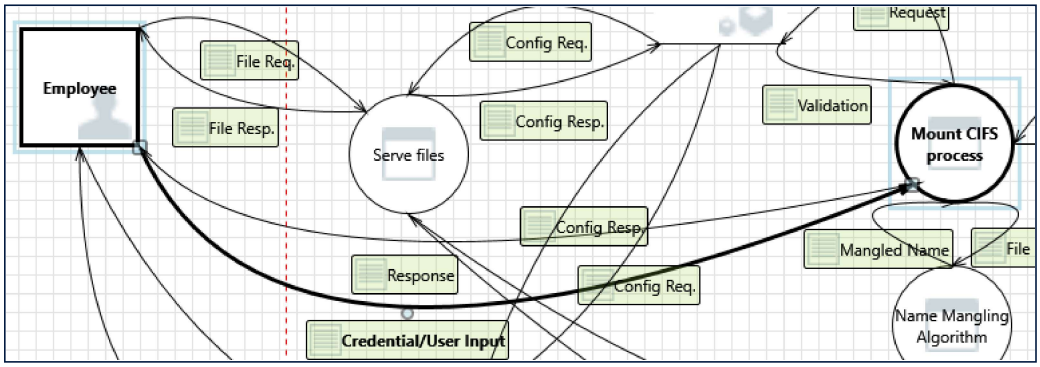
8. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of smb.conf file can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: SMB packets are encrypted

Interaction: Credential/User Input



9. Spoofing the Mount CIFS process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Mount CIFS process may be spoofed by an attacker and this may lead to information disclosure by Employee. Consider using a standard authentication mechanism to identify the destination process.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

10. Spoofing the Employee External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Employee may be spoofed by an attacker and this may lead to unauthorized access to Mount CIFS process. Consider using a standard authentication mechanism to identify the external entity.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

11. Potential Lack of Input Validation for Mount CIFS process [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Credential/User Input may be tampered with by an attacker. This may lead to a denial of service attack against Mount CIFS process or an elevation of privilege attack against Mount CIFS process or an information disclosure by Mount CIFS process. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: The Server Module Block (SMB) request protocol requires the client be authenticated to the Samba server and must be formatted in an encrypted packet

12. Potential Data Repudiation by Mount CIFS process [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Mount CIFS process claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

13. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Credential/User Input may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: SMB packets are encrypted

14. Potential Process Crash or Stop for Mount CIFS process [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Mount CIFS process crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: The OS is configures to automatically restart the samba server

15. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Samba client will reissue the request if it is interrupted

16. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Mount CIFS process may be able to impersonate the context of Employee in order to gain additional privilege.
Justification: The files are served to the employee based on employee authentication to the OS

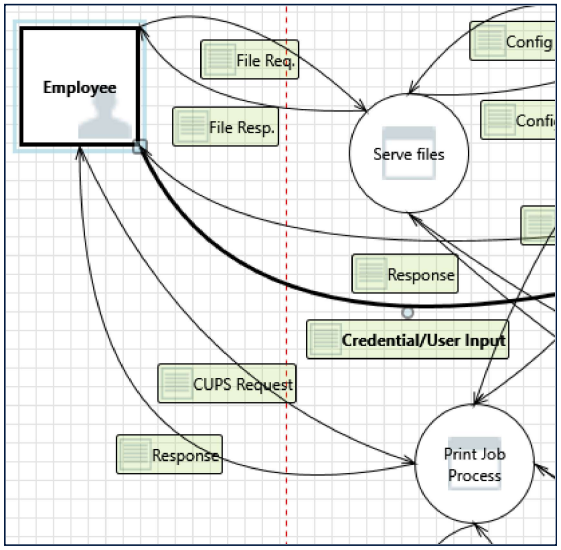
17. Mount CIFS process May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Employee may be able to remotely execute code for Mount CIFS process.
Justification: The Mount CIFS process is dependent on operating system authentication

18. Elevation by Changing the Execution Flow in Mount CIFS process [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Mount CIFS process in order to change the flow of program execution within Mount CIFS process to the attacker's choosing.
Justification: The CIFS file system mount is controlled by the OS system and is protected based on OS controls

Interaction: CUPS Request



19. Spoofing the Print Job Process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Print Job Process may be spoofed by an attacker and this may lead to information disclosure by Employee. Consider using a standard authentication mechanism to identify the destination process.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

20. Spoofing the Employee External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Employee may be spoofed by an attacker and this may lead to unauthorized access to Print Job Process. Consider using a standard authentication mechanism to identify the external entity.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

21. Potential Lack of Input Validation for Print Job Process [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across CUPS Request may be tampered with by an attacker. This may lead to a denial of service attack against Print Job Process or an elevation of privilege attack against Print Job Process or an information disclosure by Print Job Process. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: The Server Module Block (SMB) request protocol requires the client be authenticated to the Samba server and must be formatted in an encrypted packet

22. Potential Data Repudiation by Print Job Process [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Print Job Process claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

23. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across CUPS Request may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: SMB packets are encrypted

24. Potential Process Crash or Stop for Print Job Process [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Print Job Process crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: The OS is configures to automatically restart the samba server

25. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Samba client will reissue the request if it is interrupted

26. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Print Job Process may be able to impersonate the context of Employee in order to gain additional privilege.

Justification: The Print Job Process runs under the OS controls for Samba server authentication and is not able to authenticate as an employee

27. Print Job Process May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Employee may be able to remotely execute code for Print Job Process.

Justification: The Print Job Process process is dependent on operating system authentication

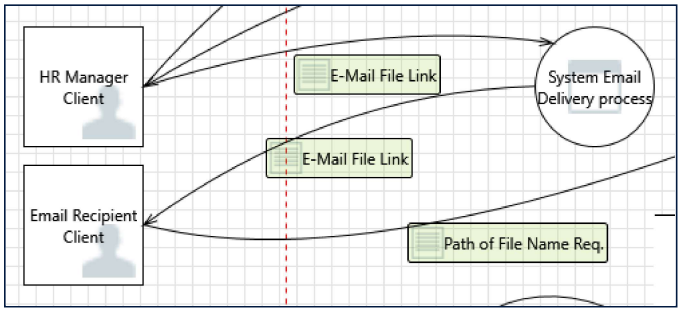
28. Elevation by Changing the Execution Flow in Print Job Process [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Print Job Process in order to change the flow of program execution within Print Job Process to the attacker's choosing.

Justification: The print system is controlled by the OS system and is protected based on OS controls

Interaction: E-Mail File Link



29. Data Flow E-Mail File Link Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Samba client will reissue the request if it is interrupted

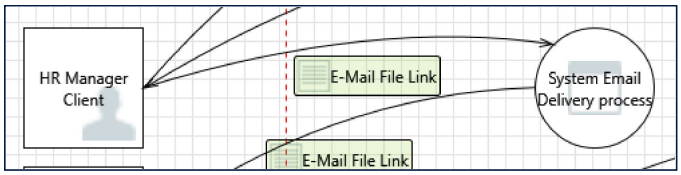
30. External Entity Email Recipient Client Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Email Recipient Client claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

31. Spoofing of the Email Recipient Client External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Email Recipient Client may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Email Recipient Client. Consider using a standard authentication mechanism to identify the external entity.
Justification: The Email Recipient Client must authenticate to the E-Mail server using POP3 or IMAP

Interaction: E-Mail File Link



32. Elevation by Changing the Execution Flow in System Email Delivery process [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into System Email Delivery process in order to change the flow of program execution within System Email Delivery process to the attacker's choosing.
Justification: The Email system delivery is an OS process which is subject to OS controls beyondthe scope of Samba

33. System Email Delivery process May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: HR Manager Client may be able to remotely execute code for System Email Delivery process.
Justification: The HR Manager client requests message delivery using the POP3 or IMAP protocols which are authenticated to the operating system

34. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: System Email Delivery process may be able to impersonate the context of HR Manager Client in order to gain additional privilege.
Justification: The System Email Delivery process uses the POP3 or IMAP protocol to deliver mesages to the HR client, which have no access to the client execution behaviour

35. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Samba client will reissue the request if it is interrupted

36. Potential Process Crash or Stop for System Email Delivery process [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: System Email Delivery process crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The OS is configures to automatically restart the samba server

37. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across E-Mail File Link may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: SMB packets are encrypted

38. Potential Data Repudiation by System Email Delivery process [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: System Email Delivery process claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

39. Potential Lack of Input Validation for System Email Delivery process [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across E-Mail File Link may be tampered with by an attacker. This may lead to a denial of service attack against System Email Delivery process or an elevation of privilege attack against System Email Delivery process or an information disclosure by System Email Delivery process. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.
Justification: The Server Module Block (SMB) request protocol requires the client be authenticated to the Samba server and must be formatted in an encrypted packet

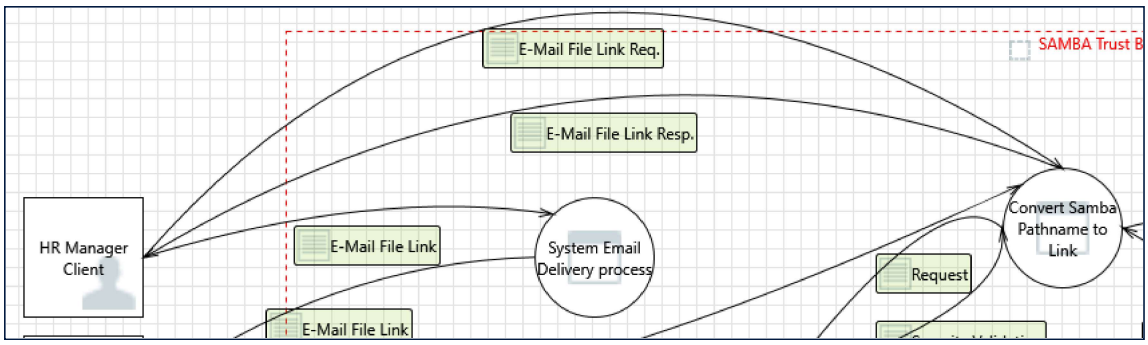
40. Spoofing the HR Manager Client External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: HR Manager Client may be spoofed by an attacker and this may lead to unauthorized access to System Email Delivery process. Consider using a standard authentication mechanism to identify the external entity.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

41. Spoofing the System Email Delivery process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: System Email Delivery process may be spoofed by an attacker and this may lead to information disclosure by HR Manager Client. Consider using a standard authentication mechanism to identify the destination process.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

Interaction: E-Mail File Link Req.



42. Spoofing the Convert Samba Pathname to Link Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Convert Samba Pathname to Link may be spoofed by an attacker and this may lead to information disclosure by HR Manager Client. Consider using a standard authentication mechanism to identify the destination process.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

43. Spoofing the HR Manager Client External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: HR Manager Client may be spoofed by an attacker and this may lead to unauthorized access to Convert Samba Pathname to Link. Consider using a standard authentication mechanism to identify the external entity.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

44. Potential Lack of Input Validation for Convert Samba Pathname to Link [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across E-Mail File Link Req. may be tampered with by an attacker. This may lead to a denial of service attack against Convert Samba Pathname to Link or an elevation of privilege attack against Convert Samba Pathname to Link or an information disclosure by Convert Samba Pathname to Link. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.
Justification: The Server Module Block (SMB) request protocol requires the client be authenticated to the Samba server and must be formatted in an encrypted packet

45. Potential Data Repudiation by Convert Samba Pathname to Link [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Convert Samba Pathname to Link claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

46. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across E-Mail File Link Req. may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: SMB packets are encrypted

47. Potential Process Crash or Stop for Convert Samba Pathname to Link [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Convert Samba Pathname to Link crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The OS is configures to automatically restart the samba server

48. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Samba client will reissue the request if it is interrupted

49. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Convert Samba Pathname to Link may be able to impersonate the context of HR Manager Client in order to gain additional privilege.
Justification: The Samba Pathname to Link cannot authenticate as a HR Manager Client without OS authentication.

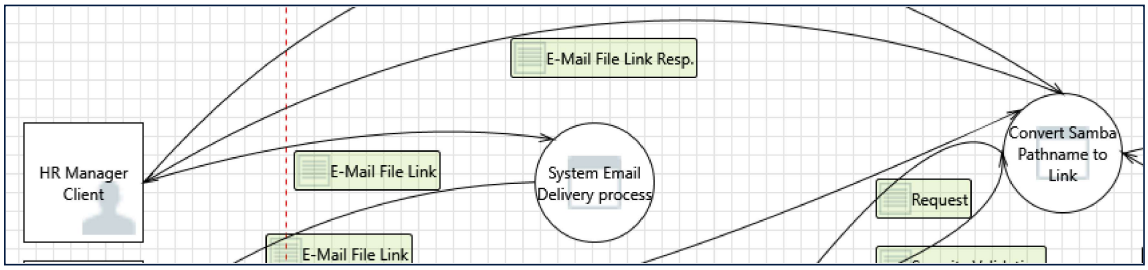
50. Convert Samba Pathname to Link May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: HR Manager Client may be able to remotely execute code for Convert Samba Pathname to Link.
Justification: Client requests including elevation of privilege are protected by the OS controls

51. Elevation by Changing the Execution Flow in Convert Samba Pathname to Link [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Convert Samba Pathname to Link in order to change the flow of program execution within Convert Samba Pathname to Link to the attacker's choosing.
Justification: The Samba demon receives SMB file access requests in an encrypted format which are not interpreted in accessing system execution paths and this is not applicable

Interaction: E-Mail File Link Resp.



52. External Entity HR Manager Client Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: HR Manager Client claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

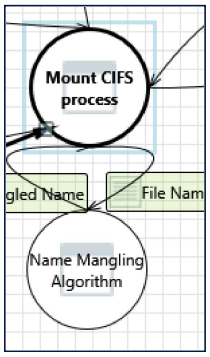
53. Spoofing of the HR Manager Client External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: HR Manager Client may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of HR Manager Client. Consider using a standard authentication mechanism to identify the external entity.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

54. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Samba client will reissue the request if it is interrupted

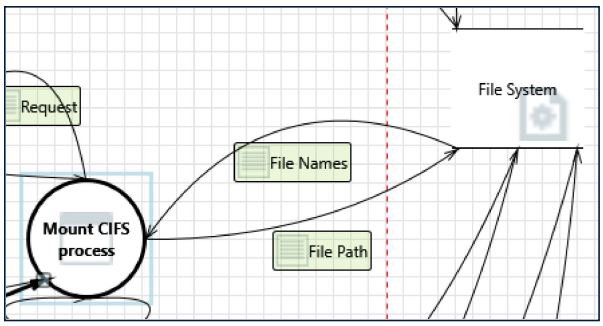
Interaction: File Name



55. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Name Mangling Algorithm may be able to impersonate the context of Mount CIFS process in order to gain additional privilege.
Justification: The Mount CIFS process is based on OS controls to validate the file system naming

Interaction: File Names



56. Spoofing of Source Data Store File System [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: File System may be spoofed by an attacker and this may lead to incorrect data delivered to Mount CIFS process. Consider using a standard authentication mechanism to identify the source data store.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

57. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of File System can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: SMB packets are encrypted

58. Spoofing the Mount CIFS process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Mount CIFS process may be spoofed by an attacker and this may lead to information disclosure by File System. Consider using a standard authentication mechanism to identify the destination process.
Justification: Users must be authenticated to the file system to access it

59. Potential Data Repudiation by Mount CIFS process [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Mount CIFS process claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

60. Potential Process Crash or Stop for Mount CIFS process [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Mount CIFS process crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The OS is configures to automatically restart the samba server

61. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The SMB protocol has retry capabilities built in

62. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent prevents access to a data store on the other side of the trust boundary.
Justification: Samba will retry and log the error

63. Mount CIFS process May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: File System may be able to remotely execute code for Mount CIFS process.

Justification: The Mount CIFS process is dependent on operating system authentication

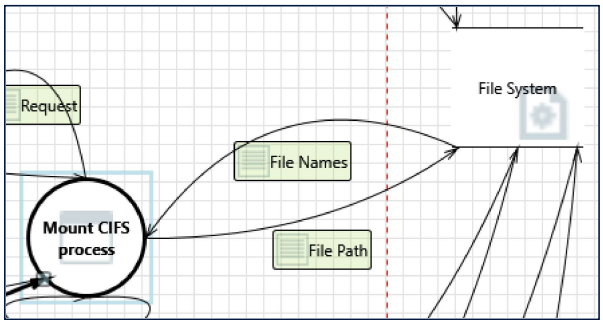
64. Elevation by Changing the Execution Flow in Mount CIFS process [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Mount CIFS process in order to change the flow of program execution within Mount CIFS process to the attacker's choosing.

Justification: The CIFS file system mount is controlled by the OS system and is protected based on OS controls

Interaction: File Path



65. Spoofing of Destination Data Store File System [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

66. Potential Excessive Resource Consumption for Mount CIFS process or File System [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Mount CIFS process or File System take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Samba operates according to the OS resource controls

67. Spoofing the Mount CIFS process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Mount CIFS process may be spoofed by an attacker and this may lead to unauthorized access to File System. Consider using a standard authentication mechanism to identify the source process.

Justification: Users must be authenticated to the file system to access it

68. The File System Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across File Path may be tampered with by an attacker. This may lead to corruption of File System. Ensure the integrity of the data flow to the data store.

Justification: The filesystem access is performed by the Samba process which is authenticated to the operating system and the file system requires a mount to the same operating system which closes the controls.

69. Data Store Denies File System Potentially Writing Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: File System claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

70. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across File Path may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: SMB packets are encrypted

71. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: The SMB protocol has retry capabilities built in

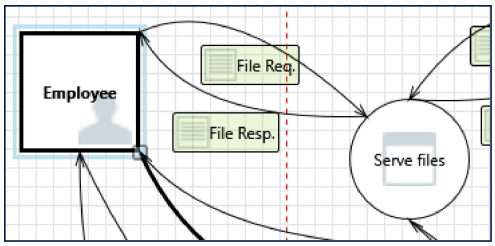
72. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Samba will retry and log the error

Interaction: File Req.



73. Elevation by Changing the Execution Flow in Serve files [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Serve files in order to change the flow of program execution within Serve files to the attacker's choosing.

Justification: The Samba daemon executes the SMB requests from the client to return file contents and does not invoke other processes

74. Serve files May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Employee may be able to remotely execute code for Serve files.

Justification: The Employee requests Samba files only using the SMB request packet which is encrypted and authenticated and cannot cause cod execution

75. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Serve files may be able to impersonate the context of Employee in order to gain additional privilege.

Justification: The files are served to the employee based on employee authentication to the OS

76. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Samba client will reissue the request if it is interrupted

77. Potential Process Crash or Stop for Serve files [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Serve files crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: The OS is configures to automatically restart the samba server

78. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across File Req. may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: SMB packets are encrypted

79. Potential Data Repudiation by Serve files [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Serve files claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

80. Potential Lack of Input Validation for Serve files [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across File Req. may be tampered with by an attacker. This may lead to a denial of service attack against Serve files or an elevation of privilege attack against Serve files or an information disclosure by Serve files. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: The Server Module Block (SMB) request protocol requires the client be authenticated to the Samba server and must be formatted in an encrypted packet

81. Spoofing the Employee External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Employee may be spoofed by an attacker and this may lead to unauthorized access to Serve files. Consider using a standard authentication mechanism to identify the external entity.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

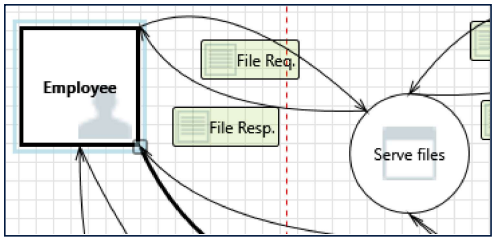
82. Spoofing the Serve files Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Serve files may be spoofed by an attacker and this may lead to information disclosure by Employee. Consider using a standard authentication mechanism to identify the destination process.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

Interaction: File Resp.



83. Spoofing of the Employee External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Employee may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Employee. Consider using a standard authentication mechanism to identify the external entity.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

84. External Entity Employee Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Employee claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

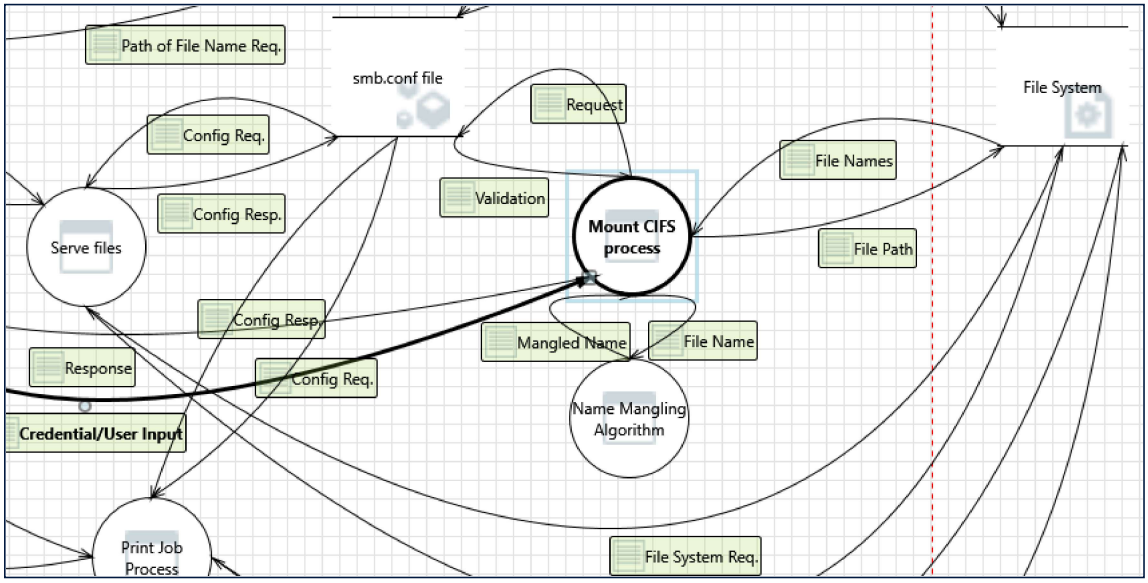
85. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Samba client will reissue the request if it is interrupted

Interaction: File System Req.



86. Spoofing of Destination Data Store File System [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

87. Potential Excessive Resource Consumption for Serve files or File System [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Serve files or File System take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Samba operates according to the OS resource controls

88. Spoofing the Serve files Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Serve files may be spoofed by an attacker and this may lead to unauthorized access to File System. Consider using a standard authentication mechanism to identify the source process.

Justification: Users must be authenticated to the file system to access it

89. The File System Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across File System Req. may be tampered with by an attacker. This may lead to corruption of File System. Ensure the integrity of the data flow to the data store.

Justification: The filesystem access is performed by the Samba process which is authenticated to the operating system and the file system requires a mount to the same operating system which closes the controls.

90. Data Store Denies File System Potentially Writing Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: File System claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

91. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across File System Req. may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: SMB packets are encrypted

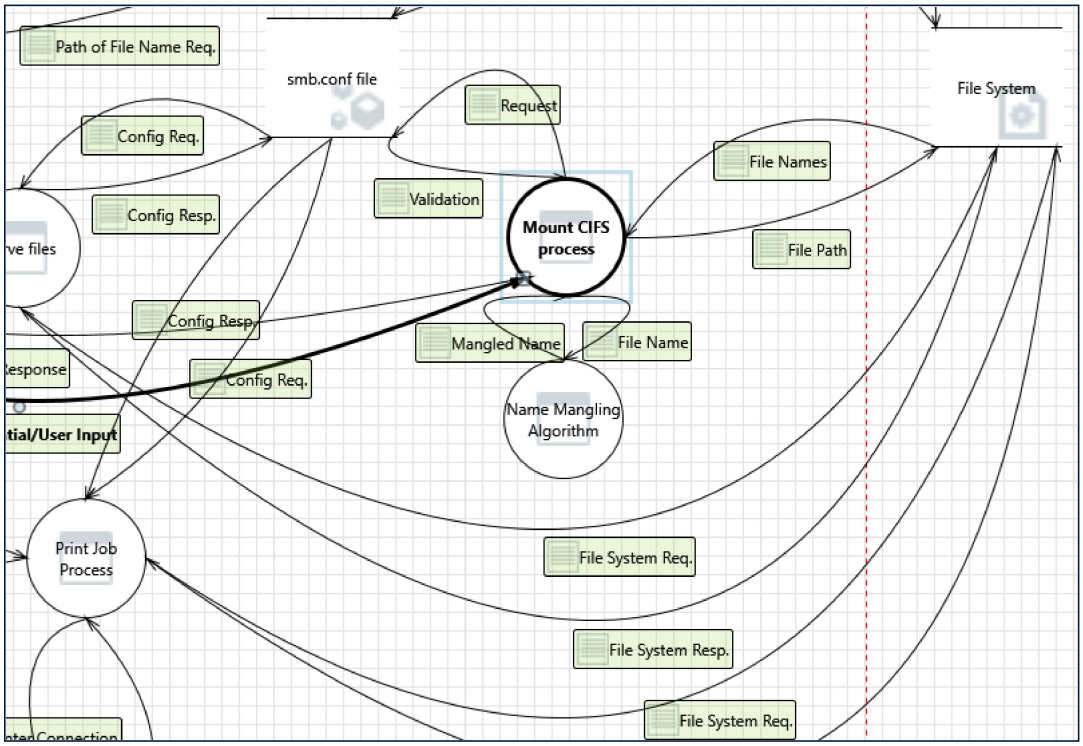
92. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The SMB protocol has retry capabilities built in

93. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent prevents access to a data store on the other side of the trust boundary.
Justification: Samba will retry and log the error

Interaction: File System Req.



94. Elevation by Changing the Execution Flow in Print Job Process [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Print Job Process in order to change the flow of program execution within Print Job Process to the attacker's choosing.
Justification: The print system is controlled by the OS system and is protected based on OS controls

95. Print Job Process May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: File System may be able to remotely execute code for Print Job Process.
Justification: The Print Job Process process is dependent on operating system authentication

96. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.
Justification: Samba will retry and log the error

97. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The SMB protocol has retry capabilities built in

98. Potential Process Crash or Stop for Print Job Process [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Print Job Process crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The OS is configures to automatically restart the samba server

99. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of File System can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: SMB packets are encrypted

100. Potential Data Repudiation by Print Job Process [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Print Job Process claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

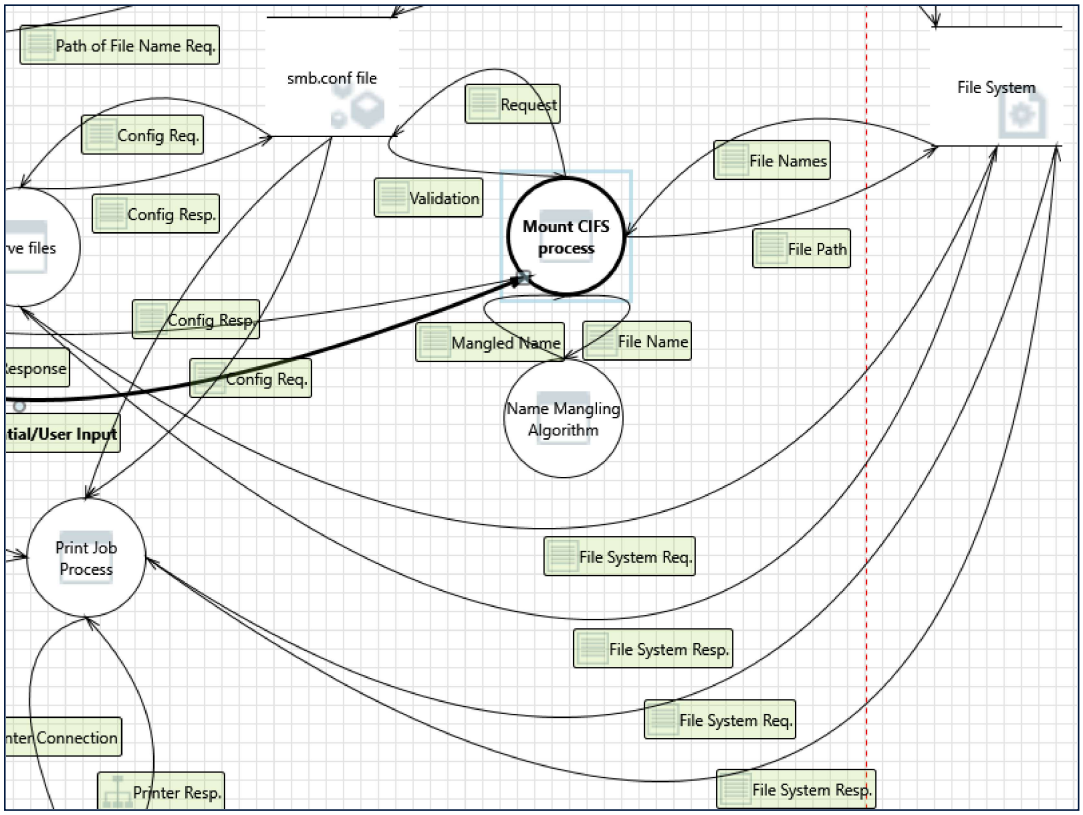
101. Spoofing of Source Data Store File System [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: File System may be spoofed by an attacker and this may lead to incorrect data delivered to Print Job Process. Consider using a standard authentication mechanism to identify the source data store.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

102. Spoofing the Print Job Process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Print Job Process may be spoofed by an attacker and this may lead to information disclosure by File System. Consider using a standard authentication mechanism to identify the destination process.
Justification: Users must be authenticated to the file system to access it

Interaction: File System Resp.



103. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent prevents access to a data store on the other side of the trust boundary.
Justification: Samba will retry and log the error

104. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: The SMB protocol has retry capabilities built in

105. Potential Excessive Resource Consumption for Print Job Process or File System [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Does Print Job Process or File System take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification: Samba operates according to the OS resource controls

106. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across File System Resp. may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: SMB packets are encrypted

107. Data Store Denies File System Potentially Writing Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: File System claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

108. The File System Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across File System Resp. may be tampered with by an attacker. This may lead to corruption of File System. Ensure the integrity of the data flow to the data store.

Justification: The filesystem access is performed by the Samba process which is authenticated to the operating system and the file system requires a mount to the same operating system which closes the controls.

109. Spoofing of Destination Data Store File System [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

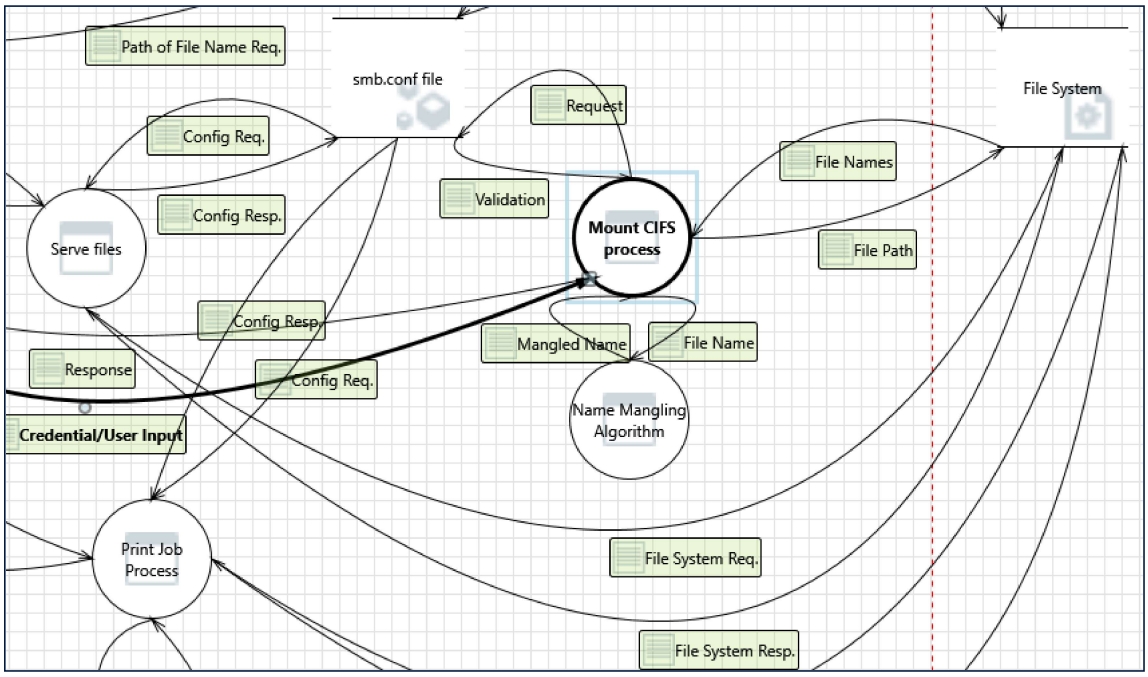
110. Spoofing the Print Job Process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Print Job Process may be spoofed by an attacker and this may lead to unauthorized access to File System. Consider using a standard authentication mechanism to identify the source process.

Justification: Users must be authenticated to the file system to access it

Interaction: File System Resp.



111. Spoofing the Serve files Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Serve files may be spoofed by an attacker and this may lead to information disclosure by File System. Consider using a standard authentication mechanism to identify the destination process.

Justification: Users must be authenticated to the file system to access it

112. Spoofing of Source Data Store File System [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: File System may be spoofed by an attacker and this may lead to incorrect data delivered to Serve files. Consider using a standard authentication mechanism to identify the source data store.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

113. Potential Data Repudiation by Serve files [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Serve files claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

114. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of File System can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: SMB packets are encrypted

115. Potential Process Crash or Stop for Serve files [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Serve files crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: The OS is configures to automatically restart the samba server

116. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: The SMB protocol has retry capabilities built in

117. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Samba will retry and log the error

118. Serve files May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: File System may be able to remotely execute code for Serve files.

Justification: The File System requests Samba files only using the SMB request packet which is encrypted and authenticated and cannot cause cod execution

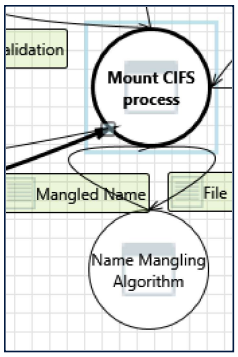
119. Elevation by Changing the Execution Flow in Serve files [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Serve files in order to change the flow of program execution within Serve files to the attacker's choosing.

Justification: The Samba daemon executes the SMB requests from the client to return file contents and does not invoke other processes

Interaction: Mangled Name



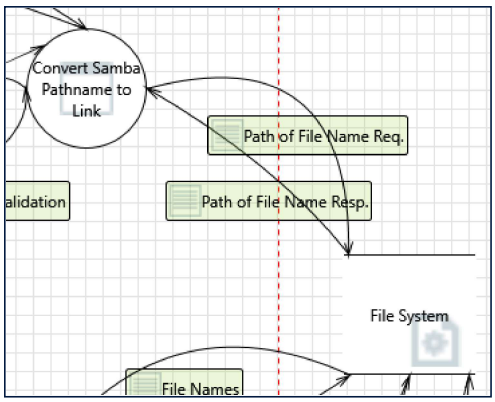
120. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Mount CIFS process may be able to impersonate the context of Name Mangling Algorithm in order to gain additional privilege.

Justification: The Mount CIFS process is based on OS controls to validate the file system naming

Interaction: Path of File Name Req.



121. Potential Excessive Resource Consumption for Convert Samba Pathname to Link or File System [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Convert Samba Pathname to Link or File System take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Samba operates according to the OS resource controls

122. Spoofing of Destination Data Store File System [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

123. Spoofing the Convert Samba Pathname to Link Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Convert Samba Pathname to Link may be spoofed by an attacker and this may lead to unauthorized access to File System. Consider using a standard authentication mechanism to identify the source process.

Justification: Users must be authenticated to the file system to access it

124. The File System Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Path of File Name Req. may be tampered with by an attacker. This may lead to corruption of File System. Ensure the integrity of the data flow to the data store.

Justification: The filesystem access is performed by the Samba process which is authenticated to the operating system and the file system requires a mount to the same operating system which closes the controls.

125. Data Store Denies File System Potentially Writing Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: File System claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

126. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Path of File Name Req. may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: SMB packets are encrypted

127. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: The SMB protocol has retry capabilities built in

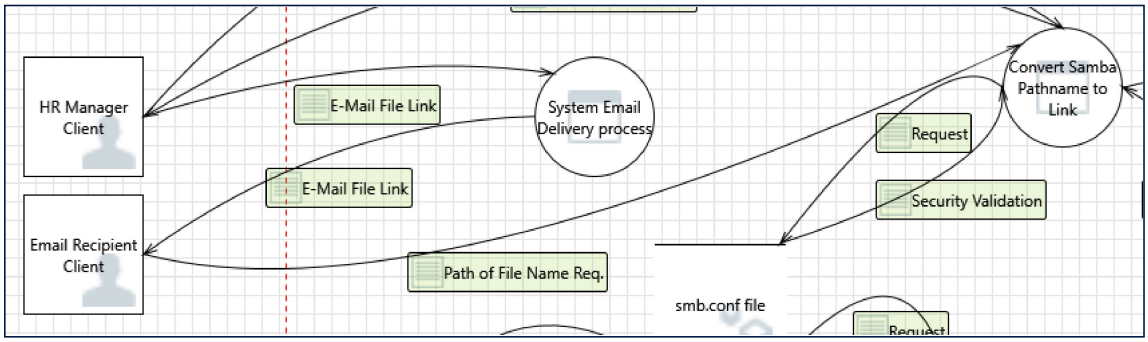
128. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Samba will retry and log the error

Interaction: Path of File Name Req.



129. Elevation by Changing the Execution Flow in Convert Samba Pathname to Link [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Convert Samba Pathname to Link in order to change the flow of program execution within Convert Samba Pathname to Link to the attacker's choosing.

Justification: The Samba demon receives SMB file access requests in an encrypted format which are not interpreted in accessing system execution paths and this is not applicable

130. Convert Samba Pathname to Link May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Email Recipient Client may be able to remotely execute code for Convert Samba Pathname to Link.

Justification: File system requests including elevation of privilege are protected by the OS controls

131. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Convert Samba Pathname to Link may be able to impersonate the context of Email Recipient Client in order to gain additional privilege.

Justification: The Samba Pathname to Link cannot authenticate as a Email Recipient Client without OS authentication.

132. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Samba client will reissue the request if it is interrupted

133. Potential Process Crash or Stop for Convert Samba Pathname to Link [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Convert Samba Pathname to Link crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: The OS is configures to automatically restart the samba server

134. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Path of File Name Req. may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: SMB packets are encrypted

135. Potential Data Repudiation by Convert Samba Pathname to Link [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Convert Samba Pathname to Link claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

136. Potential Lack of Input Validation for Convert Samba Pathname to Link [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Path of File Name Req. may be tampered with by an attacker. This may lead to a denial of service attack against Convert Samba Pathname to Link or an elevation of privilege attack against Convert Samba Pathname to Link or an information disclosure by Convert Samba Pathname to Link. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.
Justification: The Server Module Block (SMB) request protocol requires the client be authenticated to the Samba server and must be formatted in an encrypted packet

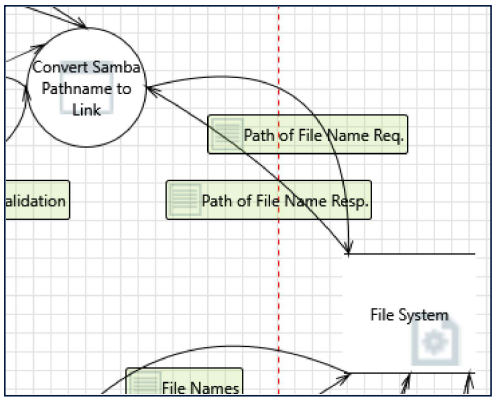
137. Spoofing the Email Recipient Client External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Email Recipient Client may be spoofed by an attacker and this may lead to unauthorized access to Convert Samba Pathname to Link. Consider using a standard authentication mechanism to identify the external entity.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

138. Spoofing the Convert Samba Pathname to Link Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Convert Samba Pathname to Link may be spoofed by an attacker and this may lead to information disclosure by Email Recipient Client. Consider using a standard authentication mechanism to identify the destination process.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

Interaction: Path of File Name Resp.



139. Spoofing of Source Data Store File System [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: File System may be spoofed by an attacker and this may lead to incorrect data delivered to Convert Samba Pathname to Link. Consider using a standard authentication mechanism to identify the source data store.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

140. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of File System can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: SMB packets are encrypted

141. Spoofing the Convert Samba Pathname to Link Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Convert Samba Pathname to Link may be spoofed by an attacker and this may lead to information disclosure by File System. Consider using a standard authentication mechanism to identify the destination process.

Justification: Users must be authenticated to the file system to access it

142. Potential Data Repudiation by Convert Samba Pathname to Link [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Convert Samba Pathname to Link claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

143. Potential Process Crash or Stop for Convert Samba Pathname to Link [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: Convert Samba Pathname to Link crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: The OS is configures to automatically restart the samba server

144. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: The SMB protocol has retry capabilities built in

145. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Samba will retry and log the error

146. Convert Samba Pathname to Link May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: File System may be able to remotely execute code for Convert Samba Pathname to Link.

Justification: File system requests including elevation of privilege are protected by the OS controls

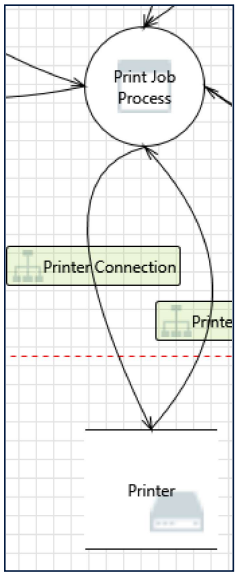
147. Elevation by Changing the Execution Flow in Convert Samba Pathname to Link [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Convert Samba Pathname to Link in order to change the flow of program execution within Convert Samba Pathname to Link to the attacker's choosing.

Justification: The Samba demon receives SMB file access requests in an encrypted format which are not interpreted in accessing system execution paths and this is not applicable

Interaction: Printer Connection



148. Spoofing of Destination Data Store Printer [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Printer may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Printer. Consider using a standard authentication mechanism to identify the destination data store.
Justification: Printer requires secure authentication as part of the print daemon setup and setup of printers requires root authentication

149. Potential Excessive Resource Consumption for Print Job Process or Printer [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Does Print Job Process or Printer take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification: Samba linits the number of print jobs

150. Spoofing the Print Job Process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Print Job Process may be spoofed by an attacker and this may lead to unauthorized access to Printer. Consider using a standard authentication mechanism to identify the source process.
Justification: Printer requires secure authentication as part of the print daemon setup and requiring operator authentication at the printer

151. The Printer Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Printer Connection may be tampered with by an attacker. This may lead to corruption of Printer. Ensure the integrity of the data flow to the data store.
Justification: CUPS printing system will restart a print job and retain integrity if a single job is corrupted

152. Data Store Denies Printer Potentially Writing Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Printer claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

153. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Data flowing across Printer Connection may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
Justification: SMB packets are encrypted

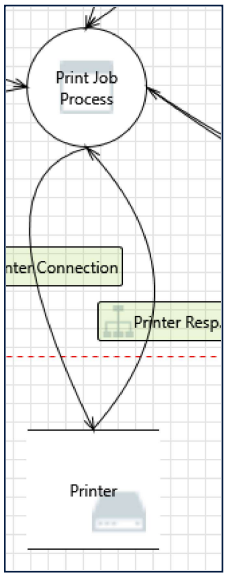
154. Data Flow UDP Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: UDP is inherentally unreliable and is used for services that can be retried

155. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent prevents access to a data store on the other side of the trust boundary.
Justification: Samba will retry and log the error

Interaction: Printer Resp.



156. Spoofing of Source Data Store Printer [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Printer may be spoofed by an attacker and this may lead to incorrect data delivered to Print Job Process. Consider using a standard authentication mechanism to identify the source data store.
Justification: Printer requires secure authentication

157. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of Printer can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: Printer communication is encrypted TLS

158. Spoofing the Print Job Process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Print Job Process may be spoofed by an attacker and this may lead to information disclosure by Printer. Consider using a standard authentication mechanism to identify the destination process.
Justification: Printer requires secure authentication as part of the print daemon setup and setup of printers requires root authentication

159. Potential Data Repudiation by Print Job Process [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Print Job Process claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

160. Potential Process Crash or Stop for Print Job Process [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Print Job Process crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: The OS is configures to automatically restart the samba server

161. Data Flow UDP Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: UDP is inherentally unreliable and is used for services that can be retried

162. Data Store Inaccessible [State: Not Applicable] [Priority: High]

Category: Denial Of Service
Description: An external agent prevents access to a data store on the other side of the trust boundary.
Justification: Accessability to the printer is not a requirement

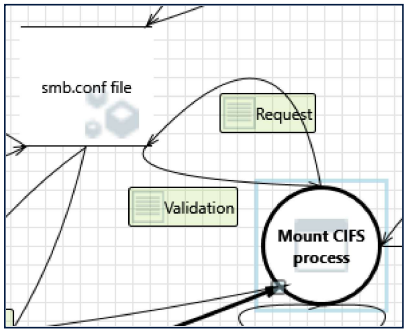
163. Print Job Process May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Printer may be able to remotely execute code for Print Job Process.
Justification: The Print Job Process process is dependent on operating system authentication

164. Elevation by Changing the Execution Flow in Print Job Process [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Print Job Process in order to change the flow of program execution within Print Job Process to the attacker's choosing.
Justification: The print system is controlled by the OS system and is protected based on OS controls

Interaction: Request



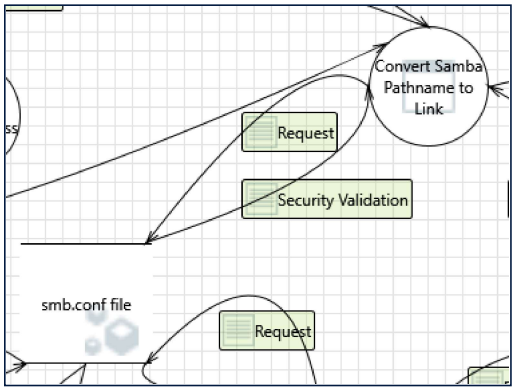
165. Potential Excessive Resource Consumption for Mount CIFS process or smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Does Mount CIFS process or smb.conf file take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification: Samba operates according to the OS resource controls

166. Spoofing of Destination Data Store smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: smb.conf file may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of smb.conf file. Consider using a standard authentication mechanism to identify the destination data store.
Justification: Smb.conf can only be in etc/Samba and only root can edit etc/

Interaction: Request



167. Spoofing of Destination Data Store smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: smb.conf file may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of smb.conf file. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Smb.conf can only be in etc/Samba and only root can edit etc/

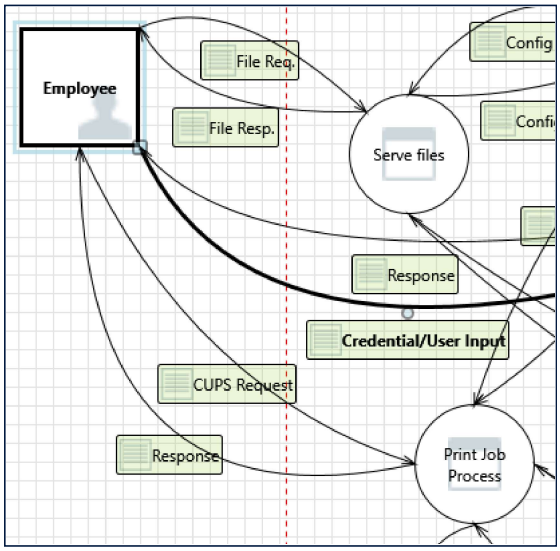
168. Potential Excessive Resource Consumption for Convert Samba Pathname to Link or smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Convert Samba Pathname to Link or smb.conf file take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Samba operates according to the OS resource controls

Interaction: Response



169. Spoofing of the Employee External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Employee may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Employee. Consider using a standard authentication mechanism to identify the external entity.

Justification: Samba requires one of 5 mehtods of user authentication to the operating system

170. External Entity Employee Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

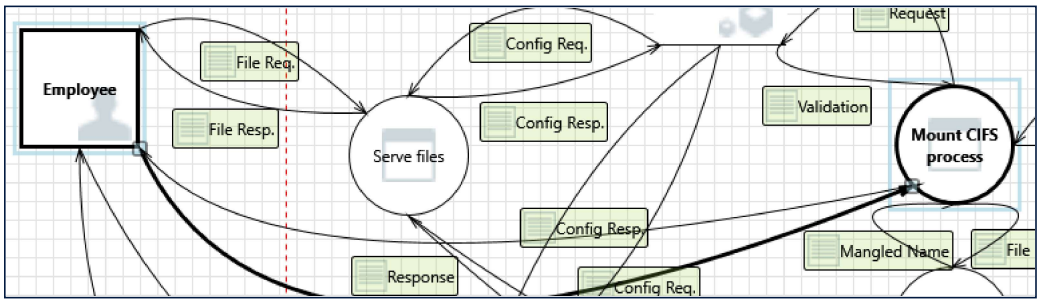
Description: Employee claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: The samba server is setup so that all events related to file access are logged

171. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Samba client will reissue the request if it is interrupted

Interaction: Response



172. Spoofing of the Employee External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Employee may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Employee. Consider using a standard authentication mechanism to identify the external entity.
Justification: Samba requires one of 5 mehtods of user authentication to the operating system

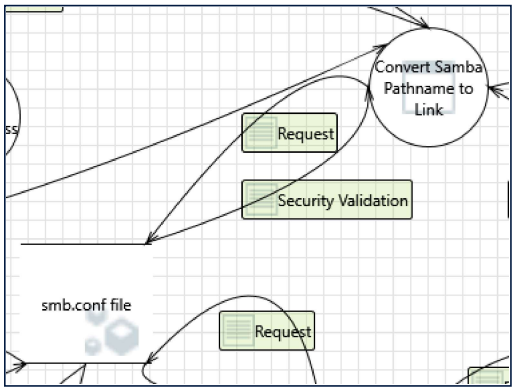
173. External Entity Employee Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Employee claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: The samba server is setup so that all events related to file access are logged

174. Data Flow SMB Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Samba client will reissue the request if it is interrupted

Interaction: Security Validation



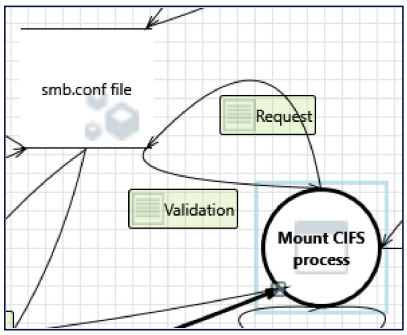
175. Spoofing of Source Data Store smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: smb.conf file may be spoofed by an attacker and this may lead to incorrect data delivered to Convert Samba Pathname to Link. Consider using a standard authentication mechanism to identify the source data store.
Justification: Smb.conf can only be in etc/Samba and only root can edit etc/

176. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of smb.conf file can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: SMB packets are encrypted

Interaction: Validation



177. Spoofing of Source Data Store smb.conf file [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: smb.conf file may be spoofed by an attacker and this may lead to incorrect data delivered to Mount CIFS process. Consider using a standard authentication mechanism to identify the source data store.
Justification: Smb.conf can only be in etc/Samba and only root can edit etc/

178. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of smb.conf file can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: SMB packets are encrypted