Threat Modeling Report

Created on 11/7/2018 10:08:56 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

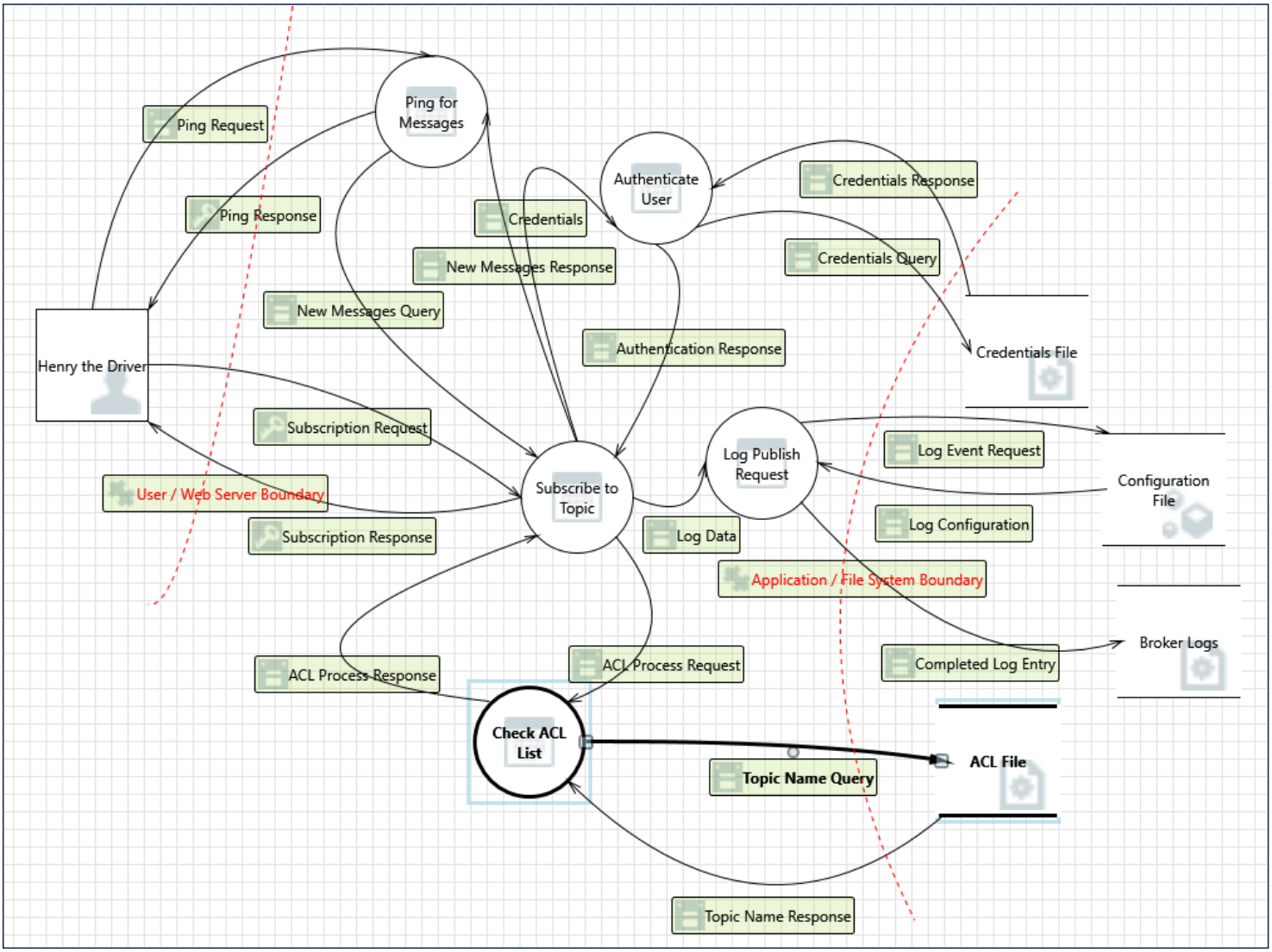
Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	21
Not Applicable	11
Needs Investigation	18
Mitigation Implemented	48
Total	98
Total Migrated	0

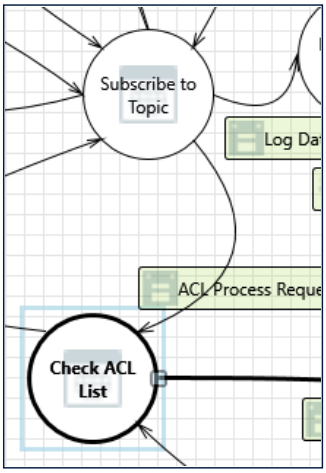
Diagram: Subscription Response



Subscription Response Diagram Summary:

Not Started	21
Not Applicable	11
Needs Investigation	18
Mitigation Implemented	48
Total	98
Total Migrated	0

Interaction: ACL Process Request



1. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Check ACL List may be able to impersonate the context of Subscribe to Topic in order to gain additional privilege.
Justification: Access type is controlled using "read", "write" or "readwrite" in the configuration file

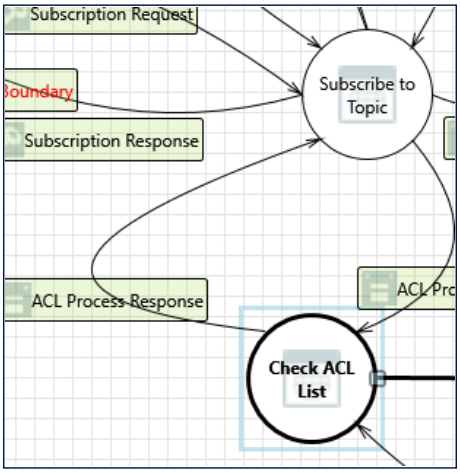
2. Spoofing the Subscribe to Topic Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Subscribe to Topic may be spoofed by an attacker and this may lead to unauthorized access to Check ACL List. Consider using a standard authentication mechanism to identify the source process.
Justification: The check is searched for the presence of either a '+' or '#' character. If either of these characters is found in either the username or client id, then the ACL check is denied.

3. Spoofing the Check ACL List Process [State: Not Applicable] [Priority: High]

Category: Spoofing
Description: Check ACL List may be spoofed by an attacker and this may lead to information disclosure by Subscribe to Topic. Consider using a standard authentication mechanism to identify the destination process.
Justification: Addressed in Level1_Subscribe_Data_Flow

Interaction: ACL Process Response



4. Elevation Using Impersonation [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege
Description: Subscribe to Topic may be able to impersonate the context of Check ACL List in order to gain additional privilege.

Justification: Requires Authentication so whatever authentication requirements exist and pre-shared-key based SSL/TLS support will be applied, salted hashes, trust boundary prevents/adds protections

5. Spoofing the Check ACL List Process [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Check ACL List may be spoofed by an attacker and this may lead to unauthorized access to Subscribe to Topic. Consider using a standard authentication mechanism to identify the source process.

Justification: Addressed in Level1_Subscribe_Data_Flow

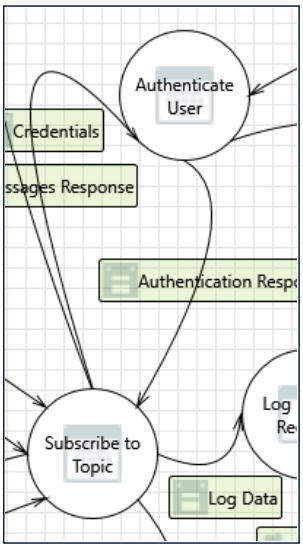
6. Spoofing the Subscribe to Topic Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Subscribe to Topic may be spoofed by an attacker and this may lead to information disclosure by Check ACL List. Consider using a standard authentication mechanism to identify the destination process.

Justification: The check is searched for the presence of either a '+' or '#' character. If either of these characters is found in either the username or client id, then the ACL check is denied.

Interaction: Authentication Response



7. Elevation Using Impersonation [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege

Description: Subscribe to Topic may be able to impersonate the context of Authenticate User in order to gain additional privilege.

Justification: Requires Authentication so whatever authentication requirements exist and pre-shared-key based SSL/TLS support will be applied, salted hashes, trust boundary prevents/adds protections

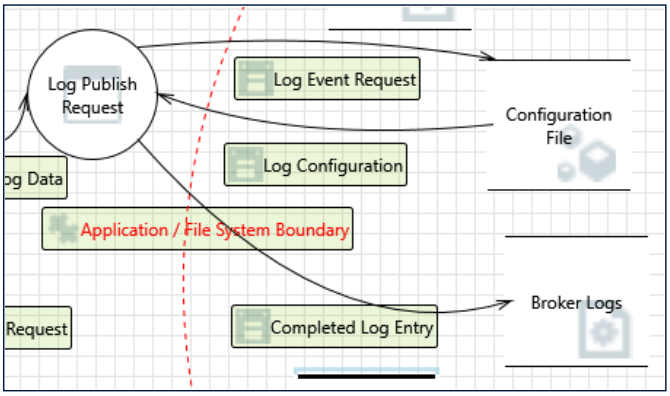
8. Spoofing the Subscribe to Topic Process [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Subscribe to Topic may be spoofed by an attacker and this may lead to information disclosure by Authenticate User. Consider using a standard authentication mechanism to identify the destination process.

Justification: Deleted action

Interaction: Completed Log Entry



9. Data Store Inaccessible [State: Not Started] [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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from accessing the data store

10. Data Flow Completed Log Entry 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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from interrupting data flow

11. Potential Excessive Resource Consumption for Log Publish Request or Broker Logs [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Does Log Publish Request or Broker Logs 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: Define the path to a file containing PEM encoded CA certificates that are trusted. Used to enable SSL communication.

12. Weak Credential Transit [State: Not Started] [Priority: High]

Category: Information Disclosure
Description: Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice.
Justification: Client ID but no User credentials are bing passed by MQTT

13. Data Flow Sniffing [State: Needs Investigation] [Priority: High]

Category: Information Disclosure
Description: Data flowing across Completed Log Entry 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: Broker logs are not currently encrypted

14. Data Store Denies Broker Logs Potentially Writing Data [State: Needs Investigation] [Priority: High]

Category: Repudiation
Description: Broker Logs 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: Currently neither stdout nor stderr logging is available

15. The Broker Logs Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Completed Log Entry may be tampered with by an attacker. This may lead to corruption of Broker Logs. Ensure the integrity of the data flow to the data store.

Justification: ACL check would prevent unauthorized access and the trust boundary protects the file system

16. Spoofing of Destination Data Store Broker Logs [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

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

Justification: Requires Authentication so whatever authentication requirements exist will be applied, trust boundary prevents/adds protections

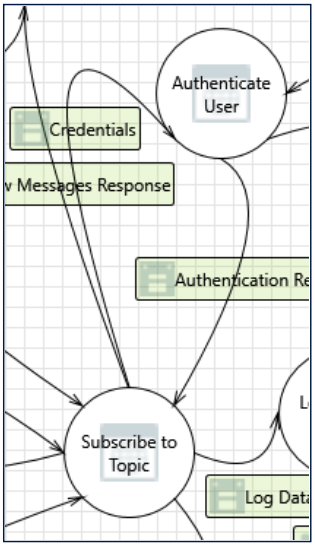
17. Spoofing the Log Publish Request Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Log Publish Request may be spoofed by an attacker and this may lead to unauthorized access to Broker Logs. Consider using a standard authentication mechanism to identify the source process.

Justification: Requires Authentication so whatever authentication requirements exist will be applied, trust boundary prevents/adds protections

Interaction: Credentials



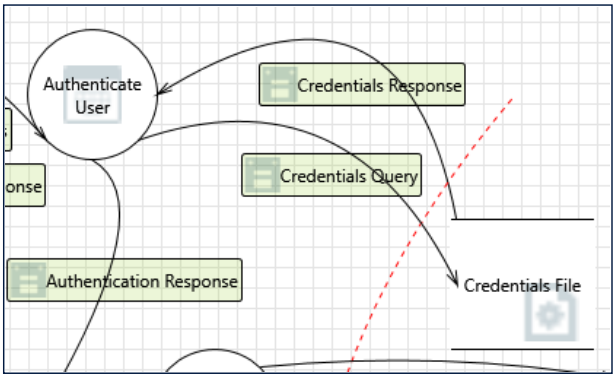
18. Elevation Using Impersonation [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege

Description: Authenticate User may be able to impersonate the context of Subscribe to Topic in order to gain additional privilege.

Justification: Requires Authentication so whatever authentication requirements exist and pre-shared-key based SSL/TLS support will be applied, salted hashes, trust boundary prevents/adds protections

Interaction: Credentials Query



19. Spoofing of Destination Data Store Credentials [State: Not Applicable] [Priority: High]

Category: Spoofing
Description: Credentials File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Credentials File. Consider using a standard authentication mechanism to identify the destination data store.
Justification: Addressed in Level1_Manage_Account_Data_Flow

20. Potential Excessive Resource Consumption for Authenticate User or Credentials [State: Not Applicable] [Priority: High]

Category: Denial Of Service
Description: Does Authenticate User or Credentials 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: Addressed in Level1_Manage_Account_Data_Flow

21. Spoofing the Authenticate User Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Authenticate User may be spoofed by an attacker and this may lead to unauthorized access to Credentials File. Consider using a standard authentication mechanism to identify the source process.
Justification: Password hashing prevents password spoofing

22. The Credentials Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Credentials Query may be tampered with by an attacker. This may lead to corruption of Credentials File. Ensure the integrity of the data flow to the data store.
Justification: Configuration would prevents buffer overflow [code lines: 155, 156, 157, 138-145] and the trust boundary protects file system

23. Data Store Denies Credentials Potentially Writing Data [State: Needs Investigation] [Priority: High]

Category: Repudiation
Description: Credentials File 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: Currently neither stdout nor stderr logging is available

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

Category: Information Disclosure
Description: Data flowing across Credentials Query 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: Requires Authentication so whatever authentication requirements exist and pre-shared-key based SSL/TLS support will be applied, salted hashes, trust boundary prevents/adds protections

25. Weak Credential Transit [State: Not Started] [Priority: High]

Category: Information Disclosure
Description: Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice.
Justification: Requires Authentication so whatever authentication requirements exist and pre-shared-key based SSL/TLS support will be applied, salted hashes, trust boundary prevents/adds protections

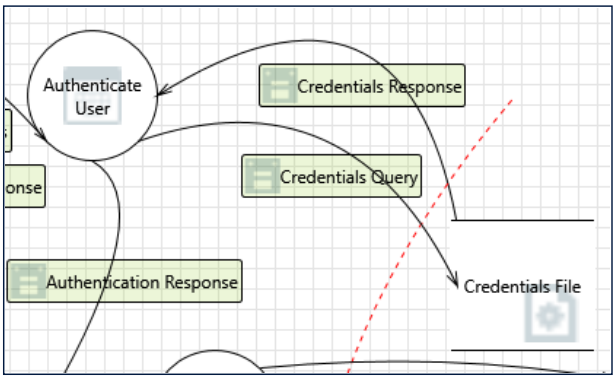
26. Data Flow Binary Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from interrupting data flow

27. Data Store Inaccessible [State: Not Started] [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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

Interaction: Credentials Response



28. Spoofing of Source Data Store Credentials [State: Not Applicable] [Priority: High]

Category: Spoofing
Description: Credentials File may be spoofed by an attacker and this may lead to incorrect data delivered to Authenticate User. Consider using a standard authentication mechanism to identify the source data store.
Justification: Addressed in Level1_Manage_Account_Data_Flow

29. Weak Access Control for a Resource [State: Not Applicable] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of Credentials File can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: Addressed in Level1_Manage_Account_Data_Flow

30. Spoofing the Authenticate User Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Authenticate User may be spoofed by an attacker and this may lead to information disclosure by Credentials File. Consider using a standard authentication mechanism to identify the destination process.
Justification: Password hashing prevents password spoofing

31. Potential Data Repudiation by Authenticate User [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Authenticate User 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: Quality of Service: request can be resent automatically until subscription ack

32. Potential Process Crash or Stop for Authenticate User [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Authenticate User crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

33. Data Flow Credentials Response 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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

34. Data Store Inaccessible [State: Not Started] [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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

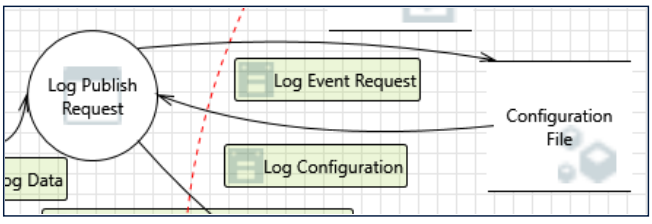
35. Authenticate User May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Credentials File may be able to remotely execute code for Authenticate User.
Justification: Addressed in Level1_Manage_Account_Data_Flow

36. Elevation by Changing the Execution Flow in Authenticate User [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Authenticate User in order to change the flow of program execution within Authenticate User to the attacker's choosing.
Justification: Requires Authentication so whatever authentication requirements exist and pre-shared-key based SSL/TLS support will be applied, salted hashes, trust boundary prevents/adds protections

Interaction: Log Configuration



37. Elevation by Changing the Execution Flow in Log Publish Request [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Log Publish Request in order to change the flow of program execution within Log Publish Request to the attacker's choosing.

Justification: Input validation

38. Log Publish Request May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Configuration File may be able to remotely execute code for Log Publish Request.
Justification: Only accessible from the host system

39. Data Store Inaccessible [State: Not Started] [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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

40. Data Flow Log Configuration 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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

41. Potential Process Crash or Stop for Log Publish Request [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Log Publish Request crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

42. Potential Data Repudiation by Log Publish Request [State: Needs Investigation] [Priority: High]

Category: Repudiation
Description: Log Publish Request 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: Currently neither stdout nor stderr logging is available

43. Spoofing the Log Publish Request Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Log Publish Request may be spoofed by an attacker and this may lead to information disclosure by Configuration File. Consider using a standard authentication mechanism to identify the destination process.
Justification: Requires Authentication so whatever authentication requirements exist will be applied, trust boundary prevents/adds protections

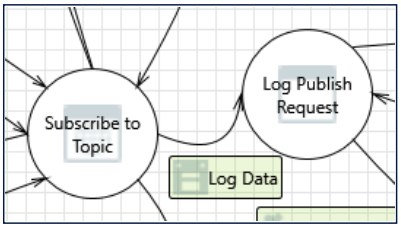
44. Weak Access Control for a Resource [State: Not Started] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of Configuration File can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: Assuming network encryption is enabled

45. Spoofing of Source Data Store Configuration File [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Configuration File may be spoofed by an attacker and this may lead to incorrect data delivered to Log Publish Request. Consider using a standard authentication mechanism to identify the source data store.
Justification: Requires Authentication so whatever authentication requirements exist will be applied, trust boundary prevents/adds protections

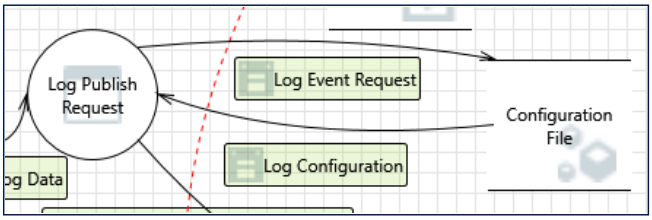
Interaction: Log Data



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

Category: Elevation Of Privilege
Description: Log Publish Request may be able to impersonate the context of Subscribe to Topic in order to gain additional privilege.
Justification: Input Validation

Interaction: Log Event Request



47. Data Store Inaccessible [State: Not Started] [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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

48. Data Flow Log Event Request 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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

49. Potential Excessive Resource Consumption for Log Publish Request or Configuration File [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Does Log Publish Request or Configuration 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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

50. Weak Credential Transit [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice.
Justification: Pre-shared-key based SSL/TLS Encryption

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

Category: Information Disclosure
Description: Data flowing across Log Event 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: Assuming network encryption is enabled

52. Data Store Denies Configuration File Potentially Writing Data [State: Needs Investigation] [Priority: High]

Category: Repudiation
Description: Configuration File 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: Currently neither stdout nor stderr logging is available

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

Category: Tampering
Description: Data flowing across Log Event Request may be tampered with by an attacker. This may lead to corruption of Configuration File. Ensure the integrity of the data flow to the data store.
Justification: ACL check would prevent unauthorized access and the trust boundary protects the file system

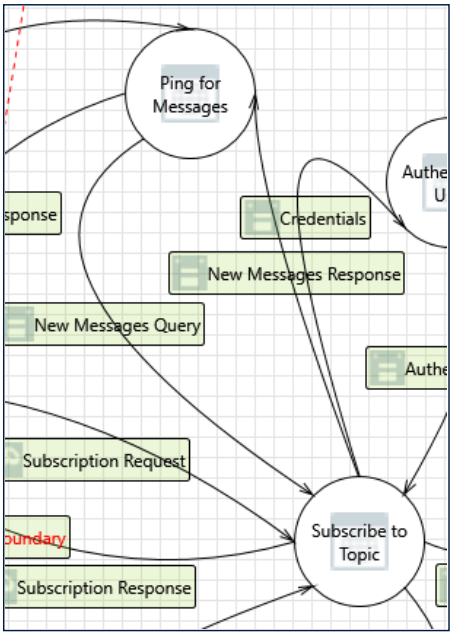
54. Spoofing of Destination Data Store Configuration File [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Configuration File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Configuration File. Consider using a standard authentication mechanism to identify the destination data store.
Justification: Requires Authentication so whatever authentication requirements exist will be applied, trust boundary prevents/adds protections

55. Spoofing the Log Publish Request Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Log Publish Request may be spoofed by an attacker and this may lead to unauthorized access to Configuration File. Consider using a standard authentication mechanism to identify the source process.
Justification: Requires Authentication so whatever authentication requirements exist will be applied, trust boundary prevents/adds protections

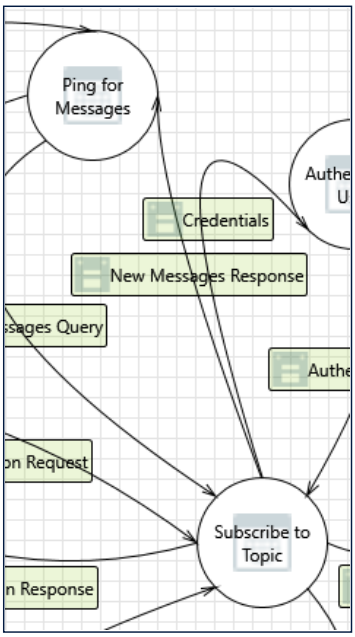
Interaction: New Messages Query



56. Elevation Using Impersonation [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege
Description: Subscribe to Topic may be able to impersonate the context of Ping for Messages in order to gain additional privilege.
Justification: Need to investigate this process further

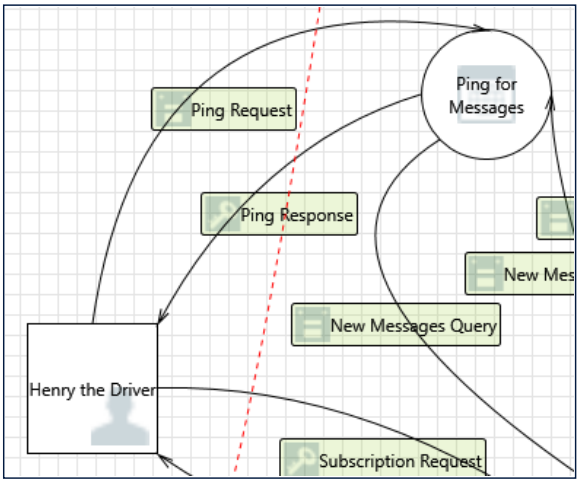
Interaction: New Messages Response



57. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Ping for Messages may be able to impersonate the context of Subscribe to Topic in order to gain additional privilege.
Justification: Both processes are running as the same user, therefore there is no chance of elevation of privilege post authentication

Interaction: Ping Request



58. Potential Process Crash or Stop for Ping for Messages [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Ping for Messages crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Number of seconds between sending PING commands to the broker for the purposes of informing it are still connected and

functioning, defaults to 60 seconds.

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

Category: Information Disclosure

Description: Data flowing across Ping 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: Pre-shared-key based SSL/TLS Encryption

60. Potential Data Repudiation by Ping for Messages [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Ping for Messages 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: Quality of Service: request can be resent automatically until subscription ack

61. Potential Lack of Input Validation for Ping for Messages [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Ping Request may be tampered with by an attacker. This may lead to a denial of service attack against Ping for Messages or an elevation of privilege attack against Ping for Messages or an information disclosure by Ping for Messages. 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: Configuration would prevents buffer overflow [file name: handle_publish.c, code lines: 155, 156, 157, 138-145] and the trust boundary protects file system

62. Spoofing the Ping for Messages Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Ping for Messages may be spoofed by an attacker and this may lead to information disclosure by Henry the Driver. Consider using a standard authentication mechanism to identify the destination process.

Justification: Requires Authentication so whatever authentication requirements exist will be applied

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

Category: Elevation Of Privilege

Description: Ping for Messages may be able to impersonate the context of Henry the Driver in order to gain additional privilege.

Justification: User credentials do not change and no input is being taken thus does not require data validation

64. Spoofing the Henry the Driver External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Henry the Driver may be spoofed by an attacker and this may lead to unauthorized access to Ping for Messages. Consider using a standard authentication mechanism to identify the external entity.

Justification: Traditional authentication combined with the certificate based SSL/TLS based options cafile/capath, certfile and keyfile.

65. Data Flow Ping Request 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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

66. Ping for Messages May be Subject to Elevation of Privilege Using Remote Code Execution [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege

Description: Henry the Driver may be able to remotely execute code for Ping for Messages.

Justification: Input Validation might mitigate this

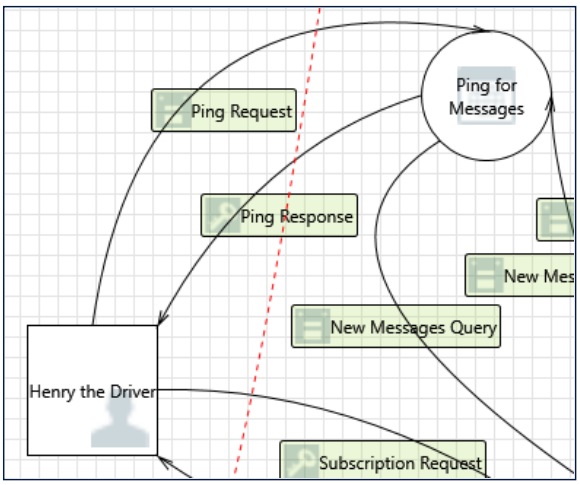
67. Elevation by Changing the Execution Flow in Ping for Messages [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege

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

Justification: Input validation

Interaction: Ping Response



68. Data Flow Ping Response 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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from interrupting data flow

69. External Entity Henry the Driver Potentially Denies Receiving Data [State: Needs Investigation] [Priority: High]

Category: Repudiation

Description: Henry the Driver 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: Quality of Service: request can be resent automatically until subscription ack

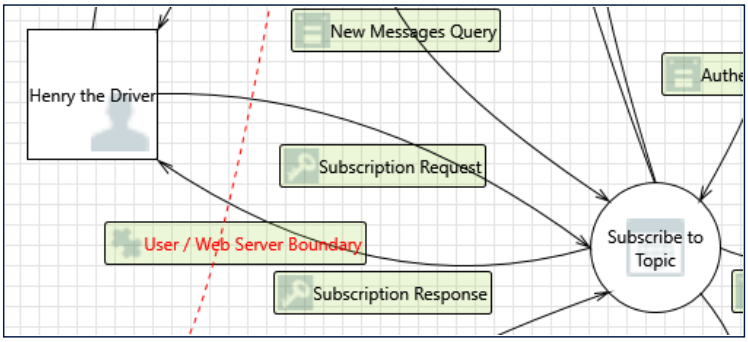
70. Spoofing of the Henry the Driver External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

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

Justification: Traditional authentication combined with the certificate based SSL/TLS based options cafile/capath, certfile and keyfile.

Interaction: Subscription Request



71. Elevation by Changing the Execution Flow in Subscribe to Topic [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Subscribe to Topic in order to change the flow of program execution within Subscribe to Topic to the attacker's choosing.
Justification: Input validation

72. Subscribe to Topic May be Subject to Elevation of Privilege Using Remote Code Execution [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege
Description: Henry the Driver may be able to remotely execute code for Subscribe to Topic.
Justification: Input Sanitation Validation might mitigate this

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

Category: Elevation Of Privilege
Description: Subscribe to Topic may be able to impersonate the context of Henry the Driver in order to gain additional privilege.
Justification: Output validation

74. Data Flow Subscription Request 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: Input Validation

75. Potential Process Crash or Stop for Subscribe to Topic [State: Needs Investigation] [Priority: High]

Category: Denial Of Service
Description: Subscribe to Topic crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Number of seconds between sending PING commands to the broker for the purposes of informing it are still connected and functioning, defaults to 60 seconds.

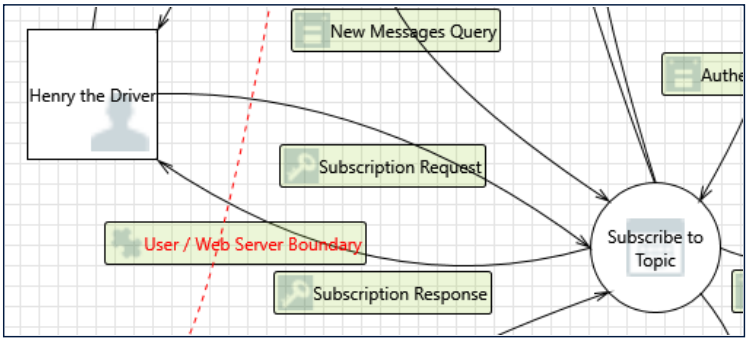
76. Potential Data Repudiation by Subscribe to Topic [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Subscribe to Topic 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: Quality of Service: request can be resent automatically until subscription ack

77. Spoofing the Henry the Driver External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Henry the Driver may be spoofed by an attacker and this may lead to unauthorized access to Subscribe to Topic. Consider using a standard authentication mechanism to identify the external entity.
Justification: Traditional authentication combined with the certificate based SSL/TLS based options cafile/capath, certfile and keyfile.

Interaction: Subscription Response



78. Data Flow Subscription Response Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from interrupting data flow

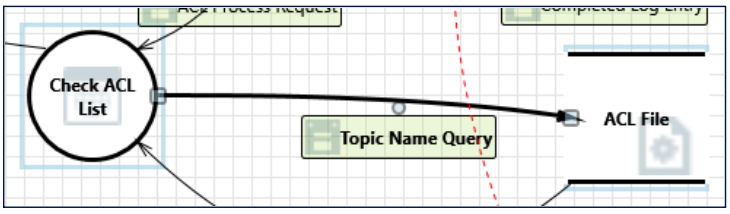
79. External Entity Henry the Driver Potentially Denies Receiving Data [State: Needs Investigation] [Priority: High]

Category: Repudiation
Description: Henry the Driver 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: Quality of Service: request can be resent automatically until subscription ack

80. Spoofing of the Henry the Driver External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Henry the Driver may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Henry the Driver. Consider using a standard authentication mechanism to identify the external entity.
Justification: Traditional authentication combined with the certificate based SSL/TLS based options cafile/capath, certfile and keyfile.

Interaction: Topic Name Query



81. Spoofing of Destination Data Store ACL File [State: Not Applicable] [Priority: High]

Category: Spoofing
Description: ACL File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of ACL File. Consider using a standard authentication mechanism to identify the destination data store.
Justification: Addressed in Level1_Subscribe_Data_Flow

82. Potential Excessive Resource Consumption for Check ACL List or ACL File [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Does Check ACL List or ACL 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: Addressed in Level1_Manage_Account_Data_Flow

83. Spoofing the Check ACL List Process [State: Not Applicable] [Priority: High]

Category: Spoofing

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

Justification: Addressed in Level1_Subscribe_Data_Flow

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

Category: Tampering

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

Justification: ACL check would prevent access to the acl file and the trust boundary protects file system

85. Data Store Denies ACL File Potentially Writing Data [State: Needs Investigation] [Priority: High]

Category: Repudiation

Description: ACL File 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: Currently neither stdout nor stderr logging is available

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

Category: Information Disclosure

Description: Data flowing across Topic Name Query 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: User would have to be on the host system and additional protections would likely be in place, trust boundary mitigates as well

87. Weak Credential Transit [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice.

Justification: Requires Authentication so whatever authentication requirements exist and pre-shared-key based SSL/TLS support will be applied, trust boundary prevents/adds protections

88. Data Flow Binary Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service

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

Justification: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from interrupting data flow

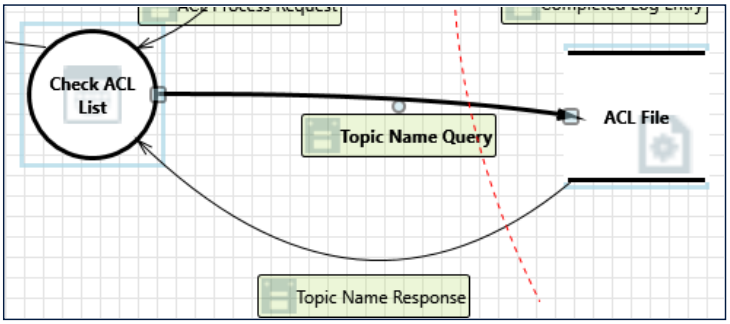
89. Data Store Inaccessible [State: Not Started] [Priority: High]

Category: Denial Of Service

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

Justification: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from interrupting data flow

Interaction: Topic Name Response



90. Spoofing of Source Data Store ACL File [State: Not Applicable] [Priority: High]

Category: Spoofing
Description: ACL File may be spoofed by an attacker and this may lead to incorrect data delivered to Check ACL List. Consider using a standard authentication mechanism to identify the source data store.
Justification: Addressed in Level1_Subscribe_Data_Flow

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

Category: Information Disclosure
Description: Improper data protection of ACL File can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: User would have to be on the host system and additional protections would likely be in place, trust boundary mitigates as well

92. Spoofing the Check ACL List Process [State: Not Applicable] [Priority: High]

Category: Spoofing
Description: Check ACL List may be spoofed by an attacker and this may lead to information disclosure by ACL File. Consider using a standard authentication mechanism to identify the destination process.
Justification: Addressed in Level1_Subscribe_Data_Flow

93. Potential Data Repudiation by Check ACL List [State: Needs Investigation] [Priority: High]

Category: Repudiation
Description: Check ACL List 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: Currently neither stdout nor stderr logging is available

94. Potential Process Crash or Stop for Check ACL List [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Check ACL List crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Returns an error when it has been set up in the configuration file

95. Data Flow Binary Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from interrupting data flow

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: Authentication using separate user accounts on either side of the trust boundary will prevent external agents from potentially locking data stores

97. Check ACL List May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: ACL File may be able to remotely execute code for Check ACL List.

Justification: Access type is controlled using "read", "write" or "readwrite" in the configuration file

98. Elevation by Changing the Execution Flow in Check ACL List [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

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

Justification: Access type is controlled using "read", "write" or "readwrite" in the configuration file