Threat Modeling Report

Created on 4/17/2024 11:49:45 AM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	30
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	30
Total Migrated	0

Diagram: Diagram 1

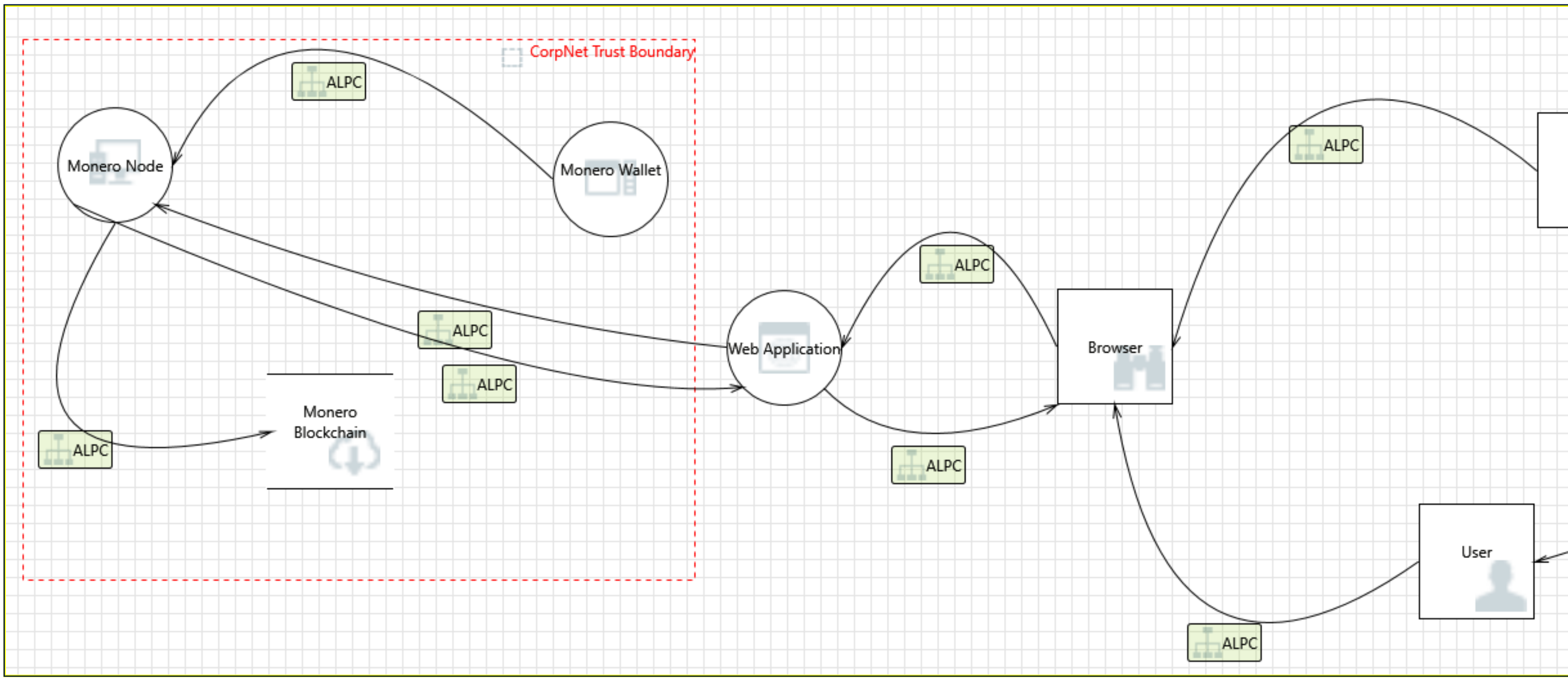
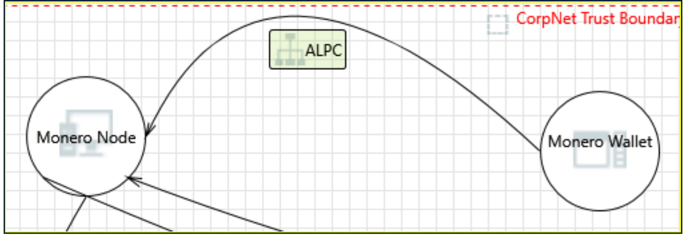


Diagram 1 Diagram Summary:

Not Started	30
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	30
Total Migrated	0

Interaction: ALPC



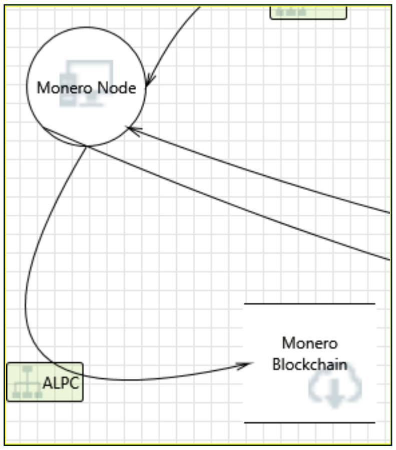
1. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering
Description: The web server 'Monero Node' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: <no mitigation provided>

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

Category: Elevation Of Privilege
Description: Monero Node may be able to impersonate the context of Monero Wallet in order to gain additional privilege.
Justification: <no mitigation provided>

Interaction: ALPC



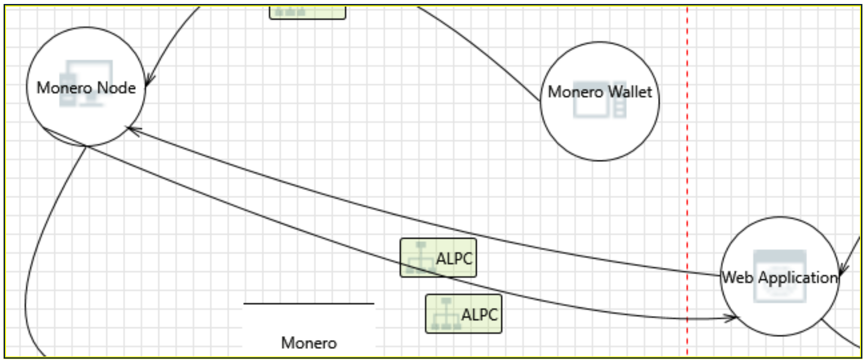
3. Spoofing of Destination Data Store Monero Blockchain [State: Not Started] [Priority: High]

Category: Spoofing
Description: Monero Blockchain may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Monero Blockchain . Consider using a standard authentication mechanism to identify the destination data store.
Justification: <no mitigation provided>

4. Potential Excessive Resource Consumption for Monero Node or Monero Blockchain [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Does Monero Node or Monero Blockchain 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: <no mitigation provided>

Interaction: ALPC



5. Monero Node May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Web Application may be able to remotely execute code for Monero Node.
Justification: <no mitigation provided>

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

Category: Elevation Of Privilege
Description: Monero Node may be able to impersonate the context of Web Application in order to gain additional privilege.
Justification: <no mitigation provided>

7. Elevation by Changing the Execution Flow in Monero Node [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Monero Node in order to change the flow of program execution within Monero Node to the attacker's choosing.
Justification: <no mitigation provided>

8. Data Flow ALPC 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: <no mitigation provided>

9. Potential Process Crash or Stop for Monero Node [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Monero Node crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: <no mitigation provided>

10. Data Flow Sniffing [State: Not Started] [Priority: High]

Category: Information Disclosure
Description: Data flowing across ALPC 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: <no mitigation provided>

11. Potential Data Repudiation by Monero Node [State: Not Started] [Priority: High]

Category: Repudiation
Description: Monero Node 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: <no mitigation provided>

12. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering
Description: The web server 'Monero Node' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: <no mitigation provided>

13. Potential Lack of Input Validation for Monero Node [State: Not Started] [Priority: High]

Category: Tampering
Description: Data flowing across ALPC may be tampered with by an attacker. This may lead to a denial of service attack against Monero Node or an elevation of privilege attack against Monero Node or an information disclosure by Monero Node. 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: <no mitigation provided>

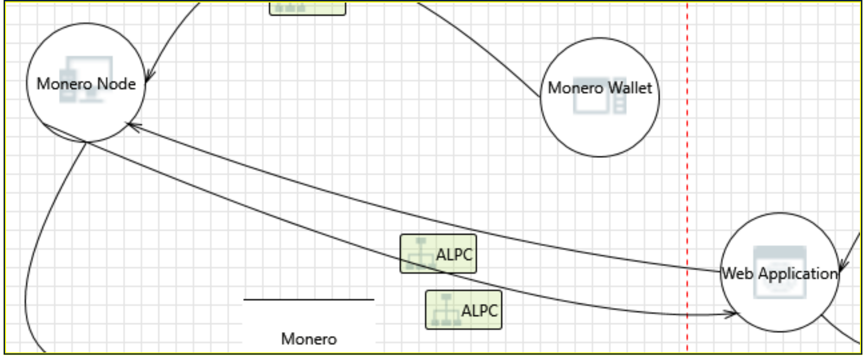
14. Spoofing the Monero Node Process [State: Not Started] [Priority: High]

Category: Spoofing
Description: Monero Node may be spoofed by an attacker and this may lead to information disclosure by Web Application. Consider using a standard authentication mechanism to identify the destination process.
Justification: <no mitigation provided>

15. Spoofing the Web Application Process [State: Not Started] [Priority: High]

Category: Spoofing
Description: Web Application may be spoofed by an attacker and this may lead to unauthorized access to Monero Node. Consider using a standard authentication mechanism to identify the source process.
Justification: <no mitigation provided>

Interaction: ALPC



16. Spoofing the Web Application Process [State: Not Started] [Priority: High]

Category: Spoofing
Description: Web Application may be spoofed by an attacker and this may lead to information disclosure by Monero Node. Consider using a standard authentication mechanism to identify the destination process.
Justification: <no mitigation provided>

17. Spoofing the Monero Node Process [State: Not Started] [Priority: High]

Category: Spoofing
Description: Monero Node may be spoofed by an attacker and this may lead to unauthorized access to Web Application. Consider using a standard authentication mechanism to identify the source process.
Justification: <no mitigation provided>

18. Potential Lack of Input Validation for Web Application [State: Not Started] [Priority: High]

Category: Tampering
Description: Data flowing across ALPC may be tampered with by an attacker. This may lead to a denial of service attack against Web Application or an elevation of privilege attack against Web Application or an information disclosure by Web Application. 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: <no mitigation provided>

19. Monero Node Process Memory Tampered [State: Not Started] [Priority: High]

Category: Tampering
Description: If Monero Node is given access to memory, such as shared memory or pointers, or is given the ability to control what Web Application executes (for example, passing back a function pointer.), then Monero Node can tamper with Web Application. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification: <no mitigation provided>

20. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering
Description: The web server 'Web Application' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: <no mitigation provided>

21. Potential Data Repudiation by Web Application [State: Not Started] [Priority: High]

Category: Repudiation
Description: Web Application 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: <no mitigation provided>

22. Data Flow Sniffing [State: Not Started] [Priority: High]

Category: Information Disclosure
Description: Data flowing across ALPC 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: <no mitigation provided>

23. Potential Process Crash or Stop for Web Application [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Web Application crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: <no mitigation provided>

24. Data Flow ALPC 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: <no mitigation provided>

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

Category: Elevation Of Privilege
Description: Web Application may be able to impersonate the context of Monero Node in order to gain additional privilege.
Justification: <no mitigation provided>

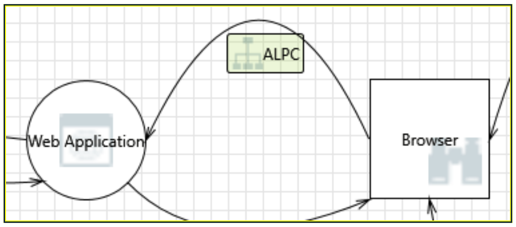
26. Web Application May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Monero Node may be able to remotely execute code for Web Application.
Justification: <no mitigation provided>

27. Elevation by Changing the Execution Flow in Web Application [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Web Application in order to change the flow of program execution within Web Application to the attacker's choosing.
Justification: <no mitigation provided>

Interaction: ALPC



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

Category: Elevation Of Privilege
Description: Web Application may be able to impersonate the context of Browser in order to gain additional privilege.
Justification: <no mitigation provided>

29. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering
Description: The web server 'Web Application' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification: <no mitigation provided>

30. Spoofing the Browser External Entity [State: Not Started] [Priority: High]

Category: Spoofing
Description: Browser may be spoofed by an attacker and this may lead to unauthorized access to Web Application. Consider using a standard authentication mechanism to identify the external entity.
Justification: <no mitigation provided>