OWASP Threat Dragon Report

Threat model diagram created with OWASP Threat Dragon

Model: Dragon_DFD

Owner: Student Mykhailenko

Reviewed by: -

Description: SCADA System for Power Plant Control and Monitoring

Diagrams

SCADA System

Description: SCADA System for Power Plant Control and Monitoring

Number of Threats: 22

Threats

1. Spoofing of Source Data Store MySQL Database

Title: Spoofing of Source Data Store MySQL Database

Type: Spoofing

Status: Open

Priority: High

Description: MySQL Database may be spoofed by an attacker and this may lead to incorrect data delivered to SCADA Server. Consider using a standard authentication mechanism to identify the source data store.

Justification: <no mitigation provided>

2. Weak Access Control for a Resource

Title: Weak Access Control for a Resource

Type: Information disclosure

Status: Open

Priority: High

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

Justification: <no mitigation provided>

3. Spoofing of Destination Data Store MySQL Database

Title: Spoofing of Destination Data Store MySQL Database

Type: Spoofing

Status: Open

Priority: High

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

Justification: <no mitigation provided>

4. Potential Excessive Resource Consumption for SCADA Server or MySQL Database

Title: Potential Excessive Resource Consumption for SCADA Server or MySQL Database

Type: Denial of service

Status: Open

Priority: High

Description: Does SCADA Server or MySQL Database 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>

5. Elevation Using Impersonation

Title: Elevation Using Impersonation

Type: Elevation of privilege

Status: Open

Priority: High

Description: PLC may be able to impersonate the context of Raspberry Server in order to gain additional privilege.

Justification: <no mitigation provided>

6. Elevation Using Impersonation

Title: Elevation Using Impersonation

Type: Elevation of privilege

Status: Open

Priority: High

Description: Raspberry Server may be able to impersonate the context of PLC in order to gain additional privilege.

Justification: <no mitigation provided>

7. Elevation Using Impersonation

Title: Elevation Using Impersonation

Type: Elevation of privilege

Status: Open

Priority: High

Description: Raspberry Server may be able to impersonate the context of SCADA Server in order to gain additional privilege.

Justification: <no mitigation provided>

8. Spoofing the Web Browser External Entity

Title: Spoofing the Web Browser External Entity

Type: Spoofing

Status: Open

Priority: High

Description: Web Browser may be spoofed by an attacker and this may lead to unauthorized access to SCADA Server. Consider using a standard authentication mechanism to identify the external entity.

Justification: <no mitigation provided>

9. Potential Lack of Input Validation for SCADA Server

Title: Potential Lack of Input Validation for SCADA Server

Type: Tampering

Status: Open

Priority: High

Description: Data flowing across Web Browser Request may be tampered with by an attacker. This may lead to a denial of service attack against SCADA Server or an elevation of privilege attack against SCADA Server or an information disclosure by SCADA Server. 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>

10. Elevation Using Impersonation

Title: Elevation Using Impersonation

Type: Elevation of privilege

Status: Open

Priority: High

Description: SCADA Server may be able to impersonate the context of Web Browser in order to gain additional privilege.

Justification: <no mitigation provided>

11. Spoofing the SCADA Server Process

Title: Spoofing the SCADA Server Process

Type: Spoofing

Status: Open

Priority: High

Description: SCADA Server may be spoofed by an attacker and this may lead to information disclosure by Web Browser. Consider using a standard authentication mechanism to identify the destination process.

Justification: <no mitigation provided>

12. Potential Lack of Input Validation for SCADA Server

Title: Potential Lack of Input Validation for SCADA Server

Type: Tampering

Status: Open

Priority: High

Description: Data flowing across Web Browser Request may be tampered with by an attacker. This may lead to a denial of service attack against SCADA Server or an elevation of privilege attack against SCADA Server or an information disclosure by SCADA Server. 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>

13. Potential Data Repudiation by SCADA Server

Title: Potential Data Repudiation by SCADA Server

Type: Repudiation

Status: Open

Priority: High

Description: SCADA Server 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>

14. Data Flow Sniffing

Title: Data Flow Sniffing

Type: Information disclosure

Status: Open

Priority: High

Description: Data flowing across Web Browser 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: <no mitigation provided>

15. Potential Process Crash or Stop for SCADA Server

Title: Potential Process Crash or Stop for SCADA Server

Type: Denial of service

Status: Open

Priority: High

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

Justification: <no mitigation provided>

16. Data Flow Generic Data Flow Is Potentially Interrupted

Title: Data Flow Generic Data Flow Is Potentially Interrupted

Type: Denial of service

Status: Open

Priority: High

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

Justification: <no mitigation provided>

17. SCADA Server May be Subject to Elevation of Privilege Using Remote Code Execution

Title: SCADA Server May be Subject to Elevation of Privilege Using Remote Code Execution

Type: Elevation of privilege

Status: Open

Priority: High

Description: Web Browser may be able to remotely execute code for SCADA Server.

Justification: <no mitigation provided>

18. Elevation by Changing the Execution Flow in SCADA Server

Title: Elevation by Changing the Execution Flow in SCADA Server

Type: Elevation of privilege

Status: Open

Priority: High

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

Justification: <no mitigation provided>

19. Cross Site Request Forgery

Title: Cross Site Request Forgery

Type: Elevation of privilege

Status: Open

Priority: High

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, … The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: <no mitigation provided>

20. Spoofing of the Web Browser External Destination Entity

Title: Spoofing of the Web Browser External Destination Entity

Type: Spoofing

Status: Open

Priority: High

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

Justification: <no mitigation provided>

21. External Entity Web Browser Potentially Denies Receiving Data

Title: External Entity Web Browser Potentially Denies Receiving Data

Type: Repudiation

Status: Open

Priority: High

Description: Web Browser 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: <no mitigation provided>

22. Data Flow Generic Data Flow Is Potentially Interrupted

Title: Data Flow Generic Data Flow Is Potentially Interrupted

Type: Denial of service

Status: Open

Priority: High

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

Justification: <no mitigation provided>

Summary

Total threats identified: 22

High priority threats: 22

Medium priority threats: 0

Low priority threats: 0

Status breakdown:

Open: 22

Mitigated: 0

Not applicable: 0

STRIDE category breakdown:

Spoofing: 5

Tampering: 1

Repudiation: 2

Information disclosure: 2

Denial of service: 3

Elevation of privilege: 9