Threat Modeling Report

Created on 11/13/2020 1:26:39 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	1
Not Applicable	8
Needs Investigation	2
Mitigation Implemented	17
Total	28
Total Migrated	0

Diagram: Diagram 1

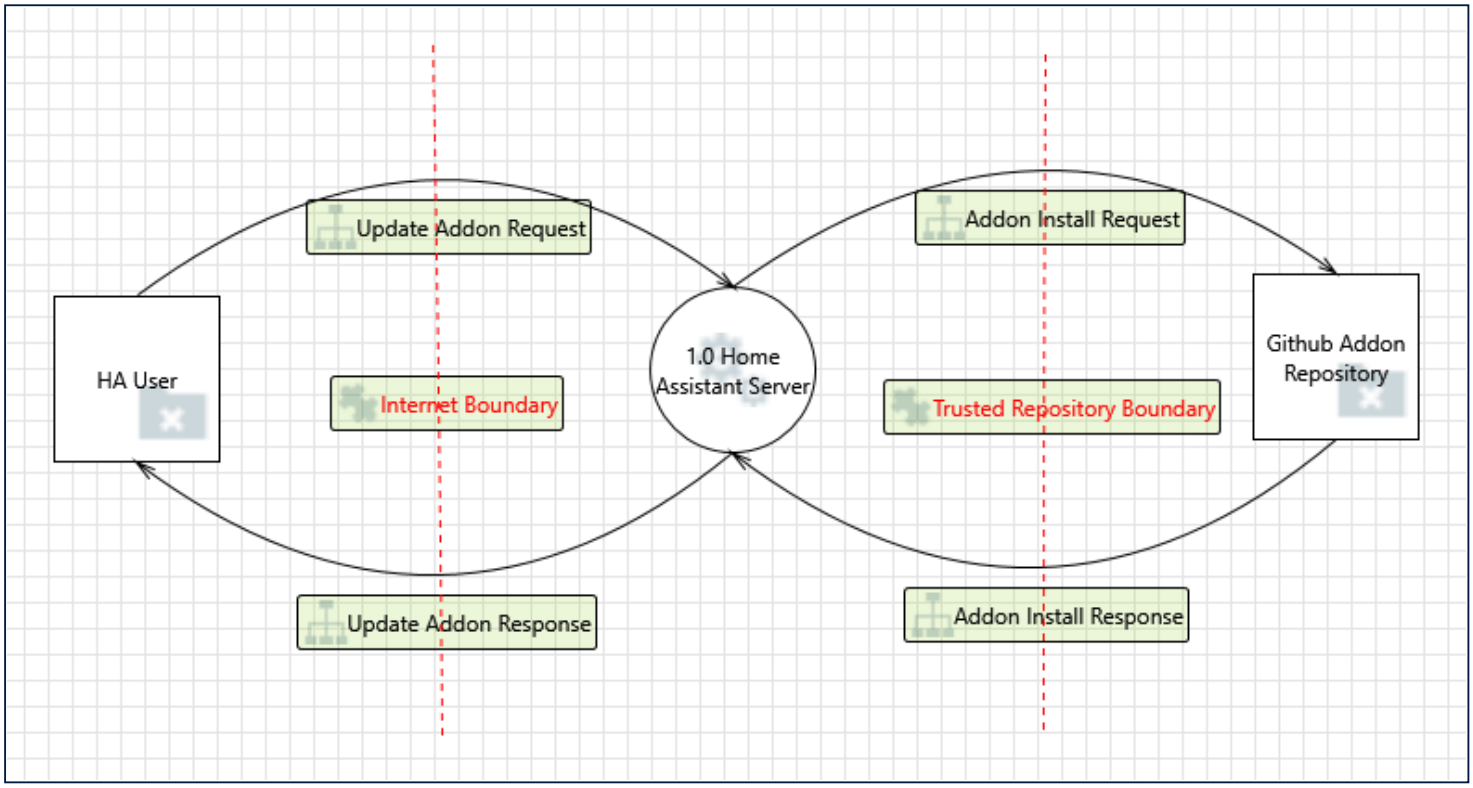
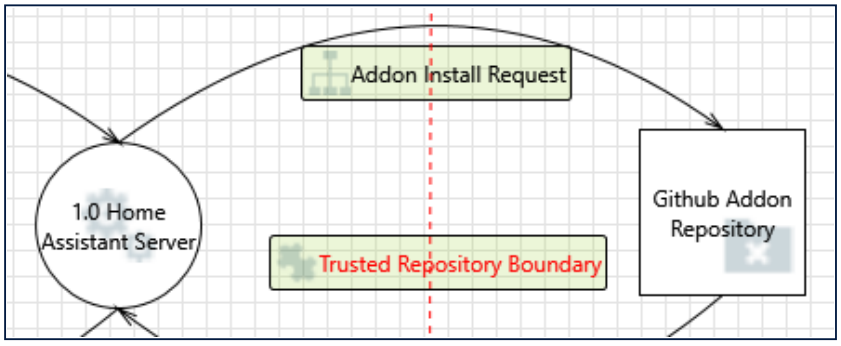


Diagram 1 Diagram Summary:

Not Started	1
Not Applicable	8
Needs Investigation	2
Mitigation Implemented	17
Total	28
Total Migrated	0

Interaction: Addon Install Request



1. Spoofing of the Github Addon Repository External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Github Addon Repository may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Github Addon Repository. Consider using a standard authentication

mechanism to identify the external entity.

Justification: The Home Assistant Server is configured to install addons from the trusted addon repository

2. External Entity Github Addon Repository Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Github Addon Repository 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: If the repository did not receive the request the user can verify this by the logs on the Home Assistant Server and resubmit the installation request.

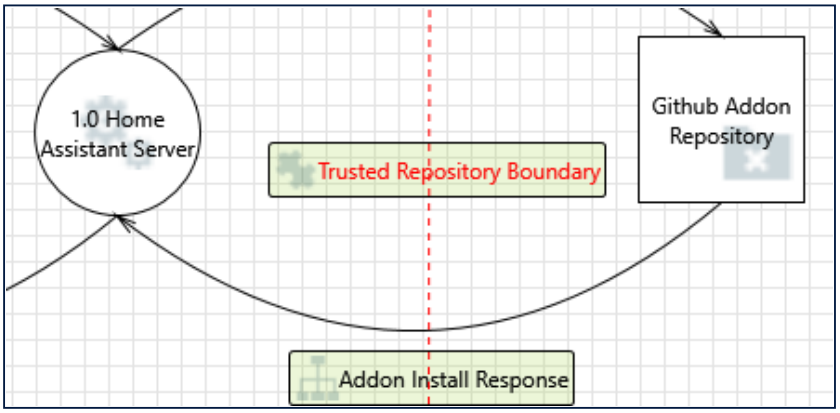
3. Data Flow Addon Install Request Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

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

Justification: If the data flow is interrupted the addon will not be installed unless the user attempts to install it again.

Interaction: Addon Install Response



4. Spoofing the Generic External Interactor External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Github Addon Repository may be spoofed by an attacker and this may lead to unauthorized access to 1.0 Home Assistant Server. Consider using a standard authentication mechanism to identify the external entity.

Justification: Home Assistant Server installs all addons with least privelge and requires a standard username/password combination for root privileges.

5. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: 1.0 Home Assistant Server may be able to impersonate the context of Github Addon Repository in

order to gain additional privilege.

Justification: Home Assistant Server installs all addons with least privelge and requires a standard username/password combination for root privileges.

6. Spoofing the 1.0 Home Assistant Server Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: 1.0 Home Assistant Server may be spoofed by an attacker and this may lead to information disclosure by Github Addon Repository. Consider using a standard authentication mechanism to identify the destination process.

Justification: Home Assistant communicates with the Github repository over HTTPS and does not send data outside of the addon install request.

7. Potential Lack of Input Validation for 1.0 Home Assistant Server [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Addon Install Response may be tampered with by an attacker. This may lead to a denial of service attack against 1.0 Home Assistant Server or an elevation of privilege attack against 1.0 Home Assistant Server or an information disclosure by 1.0 Home Assistant 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: The Home Assistant Server uses HTTPS with all trusted repositories and verifies repository checksums.

8. Potential Data Repudiation by 1.0 Home Assistant Server [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: 1.0 Home Assistant 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: Home Assistant logs all interaction with the Github addon repository, the user will be able to see a summary of the dataflow.

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

Category: Information Disclosure

Description: Data flowing across Addon Install Response 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: The only information that is sent is the Github addon file. No user information is used in this data flow.

10. Potential Process Crash or Stop for 1.0 Home Assistant Server [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: 1.0 Home Assistant Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: If the server crashs the HA user will have to re-install the addon.

11. Data Flow Addon Install 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: Home Assistant server has a list of trusted addons and communicates with GitHub over HTTPS.

12. 1.0 Home Assistant Server May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Github Addon Repository may be able to remotely execute code for 1.0 Home Assistant Server.

Justification: HA addons run in sepearte containers and run with the least privileges needed.

13. Elevation by Changing the Execution Flow in 1.0 Home Assistant Server [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 Home Assistant Server in order to change the flow of program execution within 1.0 Home Assistant Server to the attacker's choosing.

Justification: Addons installed by Home Assistant Server run in individual containers with least privilege.

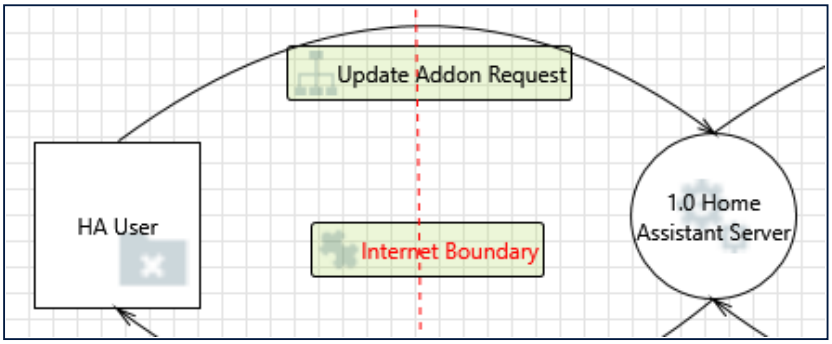
14. Cross Site Request Forgery [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege

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: Home Assistant uses HTTPS for all trusted repositories

Interaction: Update Addon Request



15. Spoofing the HA User External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: HA User may be spoofed by an attacker and this may lead to unauthorized access to 1.0 Home Assistant Server. Consider using a standard authentication mechanism to identify the external entity.

Justification: The HA user is authenticated using a standard username/password combination

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

Category: Elevation Of Privilege

Description: 1.0 Home Assistant Server may be able to impersonate the context of HA User in order to gain additional privilege.

Justification: The HA user does not have root permissions to the underlying operating system

17. Spoofing the 1.0 Home Assistant Server Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: 1.0 Home Assistant Server may be spoofed by an attacker and this may lead to information disclosure by HA User. Consider using a standard authentication mechanism to identify the destination process.

Justification: Communication between the user and the Home Assistant server is done on the local network. An attacker would have to have access to the users network in order to spoof the HA Server

18. Potential Lack of Input Validation for 1.0 Home Assistant Server [State: Not Applicable] [Priority: High]

Category: Tampering

Description: Data flowing across Update Addon Request may be tampered with by an attacker. This may lead to a denial of service attack against 1.0 Home Assistant Server or an elevation of privilege attack against 1.0 Home Assistant Server or an information disclosure by 1.0 Home Assistant 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: Data communication between the user and Home Assistant server is done over the users local network.

19. Potential Data Repudiation by 1.0 Home Assistant Server [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: 1.0 Home Assistant 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: The Home Assistant Server offers robust logging of all interaction between the user and the process.

20. Data Flow Sniffing [State: Not Applicable] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Update Addon 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: Data communication between the user and the Home Assistant Server is done over the users local network.

21. Potential Process Crash or Stop for 1.0 Home Assistant Server [State: Needs Investigation] [Priority: High]

Category: Denial Of Service

Description: 1.0 Home Assistant Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Home Assistant Server gives users the ability to create snapshots

22. Data Flow Update Addon Request Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

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

Justification: Communication between the HA User and the Server is done on the users local network.

23. 1.0 Home Assistant Server May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: HA User may be able to remotely execute code for 1.0 Home Assistant Server.

Justification: The HA user has complete control over the server and the server runs on the users local network.

24. Elevation by Changing the Execution Flow in 1.0 Home Assistant Server [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 Home Assistant Server in order to change the flow of program execution within 1.0 Home Assistant Server to the attacker's choosing.

Justification: An attacker will need to have access to the users internal network in order to spoof the user.

25. Cross Site Request Forgery [State: Not Applicable] [Priority: High]

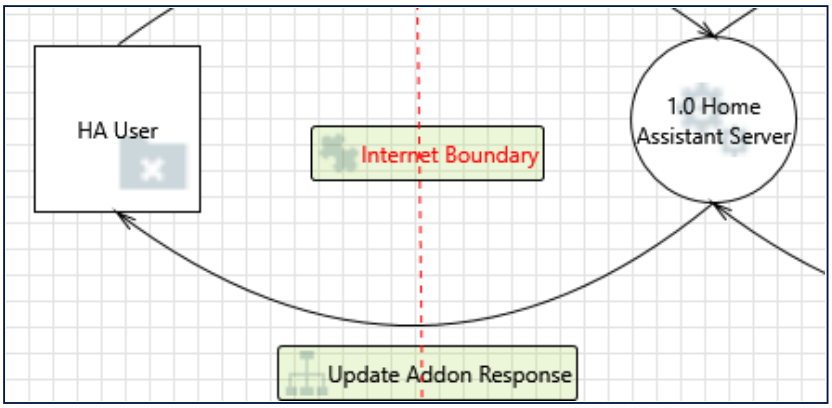
Category: Elevation Of Privilege

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: The Home Assistant server is only availble on the users local network at the static IP address assigned by the users router.

Interaction: Update Addon Response



26. Spoofing of the HA User External Destination Entity [State: Not Applicable] [Priority: High]

Category: Spoofing

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

Justification: An attacker will need to have access to the users internal network in order to spoof the user.

27. External Entity HA User Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: HA User 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 Home Assistant server offers detailed logging of all interactions regarding the user and the server.

28. Data Flow Update Addon Response Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

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

Justification: Communication between the Home Assistant Server and the user occurs on the users local network.