Threat Modeling Report

Created on 11/15/2020 8:05:08 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	1
Not Applicable	18
Needs Investigation	2
Mitigation Implemented	10
Total	31
Total Migrated	0

Diagram: Diagram 1

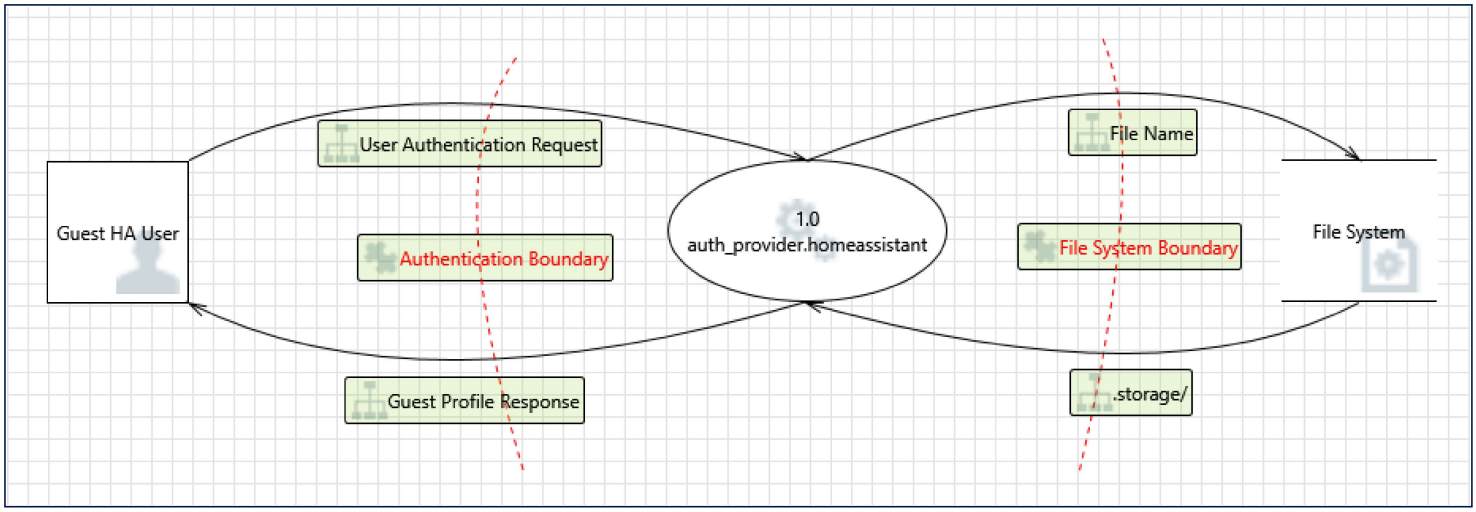
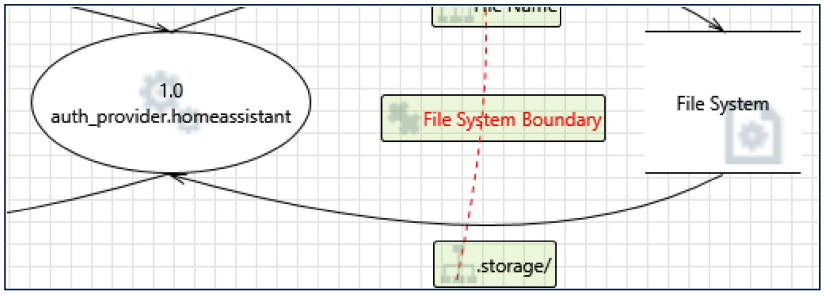


Diagram 1 Diagram Summary:

Not Started	1
Not Applicable	18
Needs Investigation	2
Mitigation Implemented	10
Total	31

Total Migrated 0

Interaction: .storage/



1. Spoofing of Source Data Store File System [State: Not Applicable] [Priority: Low]

Category: Spoofing

Description: File System may be spoofed by an attacker and this may lead to incorrect data delivered to 1.0 auth_provider.homeassistant. Consider using a standard authentication mechanism to identify the source data store.

Justification: The file systems is an internal part of the Home Assistant server which runs on the users local network. An attacker would have to get access to the users local network or have access to the device that Home Assistant runs on.

2. Weak Access Control for a Resource [State: Not Applicable] [Priority: Low]

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: The communication between auth_provider.homeassistant and the File System is happening on the Operating System. Attacker would need access to the physical device to allow for any real harm

3. Spoofing the 1.0 auth_provider.homeassistant Process [State: Not Applicable] [Priority: Low]

Category: Spoofing

Description: 1.0 auth_provider.homeassistant 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: The communication between auth_provider.homeassistant and File System is through the OS. An attacker is unable to spoof as the processes underlying Operating System.

4. Potential Data Repudiation by 1.0 auth_provider.homeassistant [State: Mitigation Implemented] [Priority: Low]

Category: Repudiation

Description: 1.0 auth_provider.homeassistant 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 Server provides detailed logging of all interactions that occur on the underlying file system.

5. Potential Process Crash or Stop for 1.0 auth_provider.homeassistant [State: Mitigation Implemented] [Priority: Low]

Category: Denial Of Service

Description: 1.0 auth_provider.homeassistant crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: If auth_provider is under any of those conditions it will still not allow faullty access to the system.

6. Data Flow .storage/ Is Potentially Interrupted [State: Not Applicable] [Priority: Low]

Category: Denial Of Service

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

Justification: Communication between auth_provider.homeassistant and the File System in done inside the OS. There is no way for an external agent to interrupt this data flow.

7. 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: Communication between auth_provider.homeassistant and the File System in done inside the OS. There is no way for an external agent to prevent access to data store. In the event the auth_provider is unable to verify credentials, this is caught inside the auth_provider process and authentication fails.

8. 1.0 auth_provider.homeassistant May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: Low]

Category: Elevation Of Privilege

Description: File System may be able to remotely execute code for 1.0 auth_provider.homeassistant.

Justification: The communication is happening through the Operating System. Remote Code execution cannot happen without attacker having direct access to physical hardware.

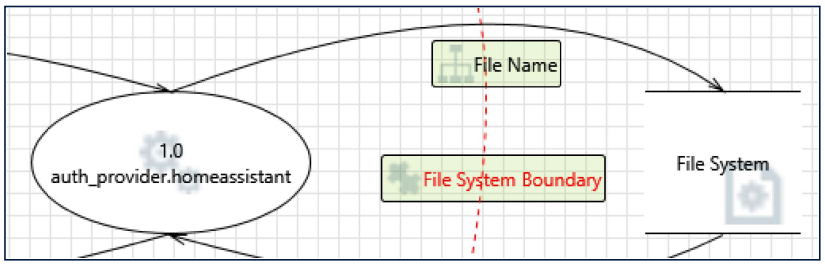
9. Elevation by Changing the Execution Flow in 1.0 auth_provider.homeassistant [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

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

Justification: Communication between auth_provider.homeassistant and the File System is happening through the Operating System. The attacker would need access to the physical system in order to execute this attack.

Interaction: File Name



10. Spoofing of Destination Data Store File System [State: Not Applicable] [Priority: Low]

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: The file systems is an internal part of the Home Assistant server which runs on the users local network. An attacker would have to get access to the users local network or have access to the device that Home Assistant runs on.

11. Potential Excessive Resource Consumption for 1.0 auth_provider.homeassistant or File System [State: Needs Investigation] [Priority: High]

Category: Denial Of Service

Description: Does 1.0 auth_provider.homeassistant 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: While the Home Assistant server itself handles deadlock, we are unsure if the auth_provider.homeassistant process has mitigations in place for this, and it is very likely as it is directly talking to the OS.

12. Spoofing the 1.0 auth_provider.homeassistant Process [State: Not Applicable] [Priority: Low]

Category: Spoofing

Description: 1.0 auth_provider.homeassistant 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: The communication between auth_provider.homeassistant and File System is through the OS. An attacker is unable to spoof as the processes underlying Operating System.

13. The File System Data Store Could Be Corrupted [State: Not Applicable] [Priority: Low]

Category: Tampering

Description: Data flowing across File Name 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: Interaction between auth_proivder and File System is handled by the Operating System. An attacker cannot tamper with the file name the process is attempting to access.

14. Data Store Denies File System Potentially Writing Data [State: Not Applicable] [Priority: Low]

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: auth_provider.homeassistant provides detailed logging of all interactions that occur with it. The file system is also not in charge of writing anything in this interaction.

15. Data Flow Sniffing [State: Not Applicable] [Priority: Low]

Category: Information Disclosure

Description: Data flowing across File Name 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 communication between auth_provider.homeassistant and the File System is happening on the Operating System. Attacker would need access to the physical device to allow for any real harm

16. Data Flow File Name Is Potentially Interrupted [State: Not Applicable] [Priority: Low]

Category: Denial Of Service

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

Justification: Communication between auth_provider.homeassistant and the File System in done inside the OS. There is no way for an external agent to interrupt this data flow.

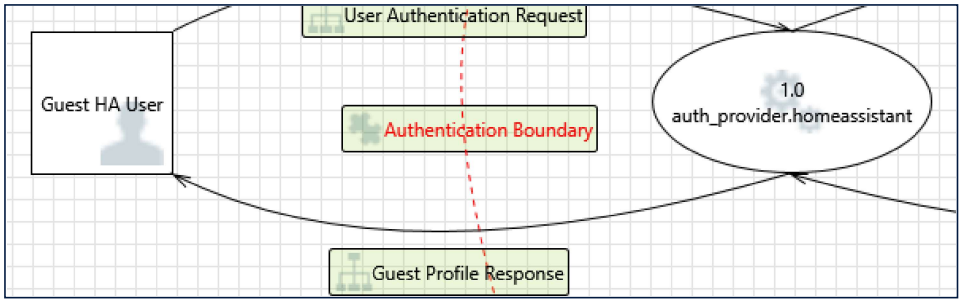
17. Data Store Inaccessible [State: Not Applicable] [Priority: High]

Category: Denial Of Service

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

Justification: Communication between auth_provider.homeassistant and the File System in done inside the OS. There is no way for an external agent to prevent access to data store. In the event the auth_provider is unable to verify credentials, this is caught inside the auth_provider process and authentication fails.

Interaction: Guest Profile Response



18. Spoofing of the Guest HA User External Destination Entity [State: Mitigation Implemented] [Priority: Low]

Category: Spoofing

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

Justification: Communication between the Guest HA User and auth_provider.homeassistant is happening on the local network. Spoofing of authentication requests is unlikely.

19. External Entity Guest HA User Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: Low]

Category: Repudiation

Description: Guest 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: auth_provider.homeassistant provides detailed logging of all interactions that occur with it.

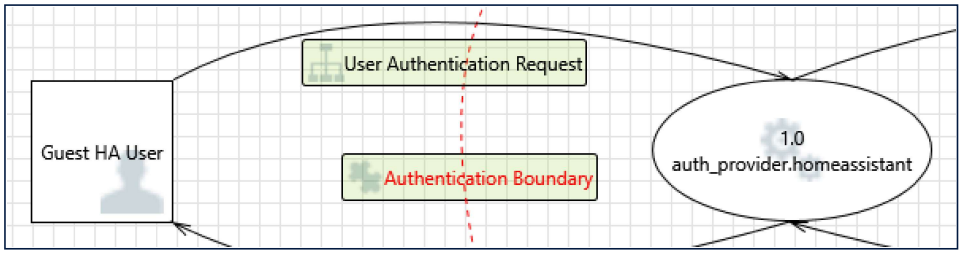
20. Data Flow Guest Profile Response Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

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

Justification: Communication between the Guest HA User and auth_provider.homeassistant process is done on the users local network.

Interaction: User Authentication Request



21. Spoofing the Guest HA User External Entity [State: Not Applicable] [Priority: Low]

Category: Spoofing

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

Justification: Users must authenticate with a username and password to obtain access to HomeAssistant, even while under local network.

22. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

Description: 1.0 auth_provider.homeassistant may be able to impersonate the context of Guest HA User in order to gain additional privilege.

Justification: Attacker would need access to the physical file system to be able to impersonate the context of Guest HA User.

23. Spoofing the 1.0 auth_provider.homeassistant Process [State: Mitigation Implemented] [Priority: Low]

Category: Spoofing

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

Justification: Communication between the Guest HA User and auth_provider.homeassistant is happening on the local network. Spoofing of authentication requests is unlikely.

24. Potential Lack of Input Validation for 1.0 auth_provider.homeassistant [State: Not Applicable] [Priority: Medium]

Category: Tampering

Description: Data flowing across User Authentication Request may be tampered with by an attacker. This may lead to a denial of service attack against 1.0 auth_provider.homeassistant or an elevation of privilege attack against 1.0 auth_provider.homeassistant or an information disclosure by 1.0 auth_provider.homeassistant. 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 request for Guest HA User is sent across the local network, and even if the request is tampered with authentication will fail.

25. Potential Data Repudiation by 1.0 auth_provider.homeassistant [State: Mitigation Implemented] [Priority: Low]

Category: Repudiation

Description: 1.0 auth_provider.homeassistant 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: auth_provider.homeassistant provides detailed logging of all interactions that occur with it.

26. Data Flow Sniffing [State: Mitigation Implemented] [Priority: Low]

Category: Information Disclosure

Description: Data flowing across User Authentication 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 flowing from Guest HA User is encrypted in transit, and is being transfered through the local network.

27. Potential Process Crash or Stop for 1.0 auth_provider.homeassistant [State: Not Started] [Priority: Low]

Category: Denial Of Service

Description: 1.0 auth_provider.homeassistant crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: If auth_provider is under any of those conditions it will still not allow faullty access to the system.

28. Data Flow User Authentication 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 Guest HA User and auth_provider.homeassistant process is done on the users local network.

29. 1.0 auth_provider.homeassistant May be Subject to Elevation of Privilege Using Remote Code Execution [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege

Description: Guest HA User may be able to remotely execute code for 1.0 auth_provider.homeassistant.

Justification: While this communication is happening via local network, meaning remote code execution is unlikely. Their still could be vulnerabilities with auth_provider that would allow this.

30. Elevation by Changing the Execution Flow in 1.0 auth_provider.homeassistant [State: Mitigation Implemented] [Priority: Low]

Category: Elevation Of Privilege

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

Justification: This communication is happening through local network, meaning attacking would be unlikely. Also, passing additional data into the auth_provider.homeassistant process will deny authentication.

31. Cross Site Request Forgery [State: Not Applicable] [Priority: Low]

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: This attack method is not valid for this communication piece. As this is the authentication verification data flow, no existing trust relationships can exist.